Health Canada Santé Canada

Canada

Privacy Technology Review

Prepared by The EXOCOM Group Inc.
Business Strategy and IT Consulting Division
for the Office of Health and the Information Highway
Health Canada
August 30, 2001

Table of Contents

Executive Summary
1 Electronic Health Records: Characteristics and U...
- 1.1 The Health Infostructure and Electronic Hea... ecords
- 1.2 Privacy Issues
- 1.3 Developing Criteria for Privacy Technology

2 Review of Privacy Technologies
- 2.1 Anonymizing Technology
- 2.2 Platform for Privacy Preferences (P3P)
- 2.3 Infomediaries and Identity Management Systems
- 2.4 Trust Management Systems
- 2.5 Smart Cards and Personal Computer Cards
- 2.6 Biometrics and Biometric Encryption
- 2.7 Public Key Infrastructure and Public Key Certificates

3 Applicability of Privacy Enhancing Technologies for Meeting Privacy requirements
- 3.1 Accountability
- 3.2 Identifying Purposes
- 3.3 Consent
- 3.4 Limiting Collection
- 3.5 Limiting Use, Disclosure, and Retention
- 3.6 Accuracy
- 3.7 Safeguards
- 3.8 Openness
- 3.9 Individual Access
- 3.10 Compliance

4 Conclusions and Recommendations
- 4.1 General
- 4.2 Unsuitable PETs
- 4.3 Useful PETs
- 4.4 Promising PETs
- 4.5 Recommendations

Annex A

Executive Summary

The EXOCOM Group Inc. assigned two principals to the project. They conducted the study and assessment from June to August 2001 in four phases, which are reflected in the organization of the document into four sections:

Section 1 - Electronic Health Records: Characteristics and Use

The authors summarized privacy requirements in the health sector, based on operational scenarios and the ten fair information practices delineated in the CSA Model Privacy Code. This phase included interviews with OHIH resources, and discussions regarding OHIH's broad concept of an electronic health record. The results are summarized in a table at the end of Section 1, which shows the ten privacy principles, the business rules that each implies, and the requirements that a privacy technology must meet to support the business rules.

Section 2 - Technology Survey

The authors surveyed commercial privacy technology available now or in the near future for supporting privacy agendas. The privacy technologies chosen are those that privacy advocates and technology vendors generally refer to as privacy enhancing technologies, as well as those that the authors determined support some aspects of privacy. The authors divided the privacy technologies into six groups or technology families, described how each is intended to address privacy, and briefly assessed its suitability in an electronic health records context in as determined by its design. At the end of each description, the authors include an abbreviated assessment table using only the ten privacy principles. The authors have noted difficulties in assessing some of the privacy technologies.

Section 3 - Technology Assessment

This section consists primarily of a detailed summary table of all six privacy technology groups, measured against the requirements developed in Section 1, and using the assessments of the technology's suitability from Section 2. This table is considerably more detailed than those in Section 2 in that the authors have added comments on the potential of a technology, when used in combination with applications or other infrastructure, to support a business rule.

Section 4 - Conclusions and Recommendations

The authors summarized the conclusions from the technology and recommend exploration of the most promising technologies, based on Section 3's results. The authors concluded that the most promising technologies are Trust Management Systems and Public Key Infrastructure, most likely in combination, and possibly using tokens. The authors recommend that OHIH undertake four activities: explore the Trust Management/Public Key Infrastructure combination in further detail; explore the use of tokens if stronger safeguards and attribution are required or if the finalized electronic health record concept includes patient control of some or all of their health record; explore the use of infomediaries if multiple identities are permitted; and develop the EHR concept concurrently with the other activities.

Annex A is a partially annotated list of useful web sites.

1 Electronic Health Records: Characteristics and Use

1.1 The Health Infostructure and Electronic Health Records

The health care sector is using technology to improve health care for Canadians wherever they are, as well as to increase the effectiveness of the health care system. Data that meets the information requirements of the health community, including individual citizens, will be part of the vision for the health info structure; data will reside in a variety of health system repositories, some of which will create data that is available to other systems, including those used for administrative support. Canada and other western nations conceive of their Electronic Health Records (EHR) systems as important elements of the health infostructure. EHRs offer the potential to meet a number of goals, and in Canada, these are summarized as follows:

- They promise to facilitate quick access for health care professionals, on a need to know basis, to an individual's health records for delivering better care;

- Individuals could have access to their health records, and will thereby be able to play a greater role in decisions about their own health care, in conjunction with health care providers[1]; and
- With appropriate safeguards, health care administrators, policy makers and researchers will be able to use integrated health care information to strengthen the health care system by reducing costs, accommodating future developments, and supporting clinical and health service research.

Some health groups have advanced the concept of the EHR as a single, longitudinal, record of an individual's encounters with health providers. In OHIH's view, an individual's EHR will be a virtual record constructed from data stored at source, or from data that resides in centralized repositories such as the proposed College of Pharmacy's provincial data collections. The patient may also have a portable record of essential personal health information that many health care providers will need, such as blood type, allergies, and adverse reactions to medication.

The health records environment uses a wide range of technology and technological capabilities, a variety of media including paper-based records, and different standards and formats for similar information. These information systems operate in and reflect the legal and regulatory differences of their jurisdictions. In order to develop a useful list of requirements that apply in most, if not all, these different environments, the authors assumed that the ideal health info structure can and will be built, and that it will be interoperable and completely electronic, as privacy enhancing technologies will be most relevant in that context.

1.2 Privacy Issues

Privacy legislation and codes are designed to provide individuals with the means to prevent exploitation of their personal information or its use in ways over which they have no control. Ultimately, privacy legislation acknowledges individual control over use of personal information, that is, over the collection, use, disclosure, retention and disposal of their information by collecting organizations. In the EHR context, the privacy requirements that are defined by the ten standard privacy principles[2] present a major challenge to the health care sector. The principles provide no guidance in terms of standards. They do provide, however, some guidance regarding business rules. A number of requirements in the ten principles remain difficult to realize in the health sector, particularly ownership of information as opposed to records that contain personal information, and the requirement to notify regarding purposes of collection, obtaining patient consent, and notification regarding changes to uses and sharing with third parties.

1.3 Developing Criteria for Privacy Technology

This report uses the business rules embedded in the ten privacy principles to establish the criteria that will be used for assessing the usefulness of technoiogies that purport to support privacy in the health care context.
The table below lists technological requirements for supporting the business rules derived from the ten privacy principles. The authors use the requirements listed in the third column of this report to assess whether or not a privacy technology or technologies supports privacy in the context of EHRs.

Principles	*Business Rules*	Requirements
1. Accountability *An organization is responsible for personal information under its*	• Appoint accountable individual • Exercise organizational responsibility within the organization	• Permit organization's accountable person to manage personal information use, disclosure etc. • Verify adherence

custody or control and shall designate an individual or individuals who are accountable for the organization's compliance with the privacy principles.	• Exercise organizational responsibility for personal information disclosed to third party(ies)	to principles e.g. audit trail • Collect/monitor status of controls used to manage other principles • Report the status of controls, assists in managing privacy issues
2. Identifying Purposes *The purposes for which personal information is collected shall be identified at or before the time the information is collected.*	• Document purposes • Notify individuals of the purpose of the collection • Notify individuals of any changes in the purpose of the collection • List data items and purposes	• Document purposes and track changes to purposes • Support accountable person • Document when and how individuals are notified of purpose and changes to purposes
3. Consent *The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information*	• Method(s) to obtain express consent for sensitive personal information • Keep track of consents - how, when, etc. • Keep track of consent withdrawals	• Document history of consent given • Audit or review consent database
4. Limiting Collection *The collection of personal information shall be limited to that which is necessary for the purposes identified. Information shall be collected by fair and lawful means*	• Describe/ document method(s) used to collect • Show source of information • Each data item must be related to purpose and substantiated • Collection of information is tailored to the stated purpose	• Document how each item supports purpose • Document how collection made • Audit or review collection • Capture explanation of why data item being collected • Capture explanation of how collection being done • Collect information according to defined rules and definitions
5. Limiting Use, Disclosure, and Retention *Personal information*	**Use:** • Reflect all purposes for each health sector provider, by sector • Identify who in health sector will use each piece	**Use:** • Document information use(s) • Document authorized access to the information;

shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.	of information • Manage access to the collection by role to avoid purpose "a" to access purpose "b" data, etc.	define the roles • Manage access based on authorization • Audit access and use • Capture who can obtain access • Permit authorized access and disallow other access • Capture / log access requests • Report access requests outside of defined authorizations
	Disclosure: • Match each access and disclosure to a purpose and document it • Manage exclusions -- XXX must not access -- and document them • Identify records that need to be kept from disclosure or use by specific groups • Some records may need special handling because they have to be treated anonymously (see HIV example)	**Disclosure:** • Deny use/ access/ receipt based on authorizations/ permissions and exclusions • Audit access/ receipt • Capture exclusions in authorization/ permissions rules • Report access/ receipt by excluded roles • Track authorized disclosures/receipts
Personal information shall be retained only as long as necessary for the fulfillment of those purposes and as required by law.	**Retention:** • At least some health records will tend to be collected and kept for extended periods of time to reflect life expectancy (100+ years) • Retention agreements as per Consent • Disposal of records and backups • Record of disposal • Reliable disposal/ destruction	**Retention:** • Document rules for retention • Document information disposal • Audit disposal of all information in a collection • Audit destruction and verify • Capture, hold, manage records for long retention periods • Inventory all copies (backups, all subsets, all media) • Document/ capture all steps in collection's life cycle
6. Accuracy *Personal information*	• Data validation procedures • Integrity maintenance • Link to openness.	• Defined accuracy and maintenance

shall be accurate and as up-to-date as necessary to fulfill the purposes for which it is collected.	(See also 9. Individual Access to information, and ability to correct information, below)	checks • Integrity designed into collection and retention mechanisms, across collections (See also 9 below)
7. Safeguards *Security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification, through all phases of its life cycle, regardless of the format in which it is held*	• Define security requirements according to sensitivity of information, impact of loss/compromise/corruption • Base needs on an accepted TRA process • Validate against a known "Best Practice" standard e.g. ISO17799 • Need supporting info showing WHY each safeguard is needed - or not • Issues re safeguards for very long term holdings (100+ years) • Software and hardware will need to become part of the "record" because they are needed to read the info	• Information protection due diligence • Accepted security practices (standards) • Confidentiality and integrity objectives considered high • Right to access very limited • Safeguards selection based on requirements • Approach can be HAZOP[3], ISO17799, Cobit or other recognized standard • Specific data protection tools justified to meet objectives • For long-lived records, must allow for retrieval across generations of technology: software and hardware can become part of the record so that the record can be read throughout its life
8. Openness *Specific information about policies and practices relating to the management of personal information shall be made readily available.*	• Policy manual becomes a public document • Policy changes are public information because of the need to inform • Need to manage public versus proprietary components	• Mechanism(s) for policy accessibility
An individual shall be informed of the existence, use and disclosure	• Inform about existence, use, disclosure • Need a process for informing individuals about the status of the collection	• Mechanisms for individual to receive/ access status of information

of his or her personal information.	(see 2., 3. and 4.) • Need to keep track of who has been or who cannot be informed • Need to track use for reporting to individuals. Where has information been used and by who and for what purpose • Need to track other disclosures for reporting to individuals • Need to track when information has been destroyed	including use, disclosure (includes who has access to the information), disposal • Mechanisms to track collection, use, disclosure, consents, disposal
9. Individual Access *Upon request, an individual shall be given access to his or her personal information. Exceptions to the right of access must be limited and specific.*	• Document exceptions • Methods for granting access to information owner • Methods for verifying identity of individuals	• Permit individuals to access their information; block exceptions (identification and authentication) • Record who requests, how, when
An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.	• Track reasons for any change with before/after cases • Document time limits if applicable • Track when individual has been given access and of the results of this access • Need for other supporting evidence	• Reliable change management process to record requests, action them, track changes and confirm them to the individual making the request • Mechanism for propagating the change across all copies of collections that include the individual's information
10. Challenging Compliance *An individual shall be able to address a challenge concerning compliance with privacy requirements to a designated individual or individuals.*	• Document compliance challenge process, including response mechanisms and accountabilities • Method to respond to challenge, manage challenges • Document the process for amending privacy practices	• Audit compliance challenges and responses

2 Review of Privacy Technologies

Privacy Technologies must provide tools that will allow organizations to manage their approach to privacy for both their staffs and for the individuals from whom they collect information. Our approach in this assessment has been to identify the characteristics or functions that automated tools should have in order to support privacy principles and objectives. Section 1 of this report identifies those requirements.

EHR systems are designed to collect health information. By default, most of that information is about individuals and has to be managed and processed according to the well-recognized Privacy Principles. These privacy requirements are distinct from the requirements to be met for the management of the health information in EHRs.

Privacy Technologies, or Privacy Enhancing Technologies (PETs),[4] as generally defined in WWW searches, have directed themselves primarily to protecting an individual's identity during visits to web sites, web interactions and web transactions. While this type of tool for creating anonymity may have a role in how individuals have access to health information, they may not be appropriate in environments where data about a person must be clearly linked to specific individuals and where access must be limited to authorized parties. This is true of EHRs, where creating, altering, sharing, communicating and destroying data about an individual's health need to be attributed to and limited to authorized individuals.

Other approaches are emerging. Some, such as smart cards, are new ways to use existing security technology to enhance privacy. This section contains descriptions of what is currently understood to be privacy related technologies and their capability or potential to support privacy-related rules. It is also important to note that technology can be used to support policies, processes and procedures, but is not a substitute for them.

This section identifies six major categories of Privacy Technologies. Each group is described below with a summary assessment of how this technology can or cannot support privacy. Annex A is a partially annotated bibliography of PET web sites. The tables in this section accompanying the assessment of each technology address whether or not, at a macro level, the technology design can support privacy business rules. For some technologies, the capacity to address a privacy requirement will depend on EHR design and the role the patient will play in controlling their personal information. Section 3 is a more detailed analysis of the technology's potential to support privacy business rules.

↑

2.1 Anonymizing Technology

Anonymity is defined as lack of identity. Anonymizers replace the identity of Internet users with a temporary identifier that exists only for the duration of the access. By doing so, any personal information the individual provides cannot be traced back to them.

Anonymizers operate on the concept that threats to an individual's privacy on the Internet derive from unauthorized monitoring of on-line actions, unknown logging of on-line actions, preservation of those logs for future access, and disclosure of the collected information to unknown parties. Monitoring and logging across multiple Internet sites can create vast amounts of information that can be aggregated and manipulated for various uses, all unknown to the individual. Individuals thereby lose the ability to choose what they want to disclose about themselves and the destination and use of their information and activities. Anonymity offers an Internet user the ability to visit web sites and conduct transactions without revealing who they really are and what their interests are. In that sense, any information collected about their WWW habits loses most of its meaning.

On the Internet, anonymity can take the form of persistent anonymity, or pseudonymity, where the user has a persistent on-line persona not connected to their real name; and one-time

anonymity, where the user has an on-line persona that lasts for one use. In both cases, the information cannot be linked to a user's real name, although in the case of pseudonymity, various on-line actions can be linked to that pseudonym. Simple anonymizing techniques include using a third party that deletes Internet message headers and resends the message content using their identifier, or connecting to a mail server and forging fake headers that are attached to the message body. Anonymous re-mailers combine these two techniques by using a computer to automate the header stripping and resending process. In most cases, there is a location on someone's system that links the pseudonym to the real user, so security controls are needed to protect this link. Re-mailers vary in the strength of protection provided for this pseudonym.

Trusted intermediaries and technologies can minimize the need to collect personal information, or minimize the number of times the information needs to be accessed. New re-mailer technology gives enhanced protection against eavesdropping through techniques such as chaining and encryption of each link of the chain, and constant-length messages. Some can defend against replay attacks and passive correlation attacks, and use continuously generated random traffic to hide real messages. Pseudonymity servers deliver additional anonymity by using pools of re-mailer identities and encryption. Message pools protect users by allowing them to encrypt their message with the recipient's public key and send the message to a mailing list or newsgroup. Re-mailers can also be used for anonymous Web browsing: a web proxy can filter out identifying headers and source addresses from a web browser.

For electronic commerce, privacy and identity protection technology is promising, and anonymous digital cash, such as DigiCash's ecash, uses cryptography to protect a payee's identity and thus accords privacy. It is likely that designing anonymity into various services will move towards infrastructures that support bi-directional anonymity, analogous to a re-mailer network, and sometimes referred to as "Pipenet". To date, Pipenet designs have insufficient protection against the traditional attacks that can be made on re-mailers and that are associated with low-latency, long-lived connections. Some Internet credit card systems, however, allow individuals to make a credit card purchase over the Internet without transferring card numbers directly to the vendor.

Assessment of Anonymizing Technologies:

For virtual EHRs, anonymizing technology has limited potential, particularly given current vulnerability to attacks. Anonymous credit card transaction methodology may help to address authorizations for payment for health services, if that is considered part of an EHR. The underlying assumptions for anonymizing technology are in fact contrary to some EHR requirements: Anonymizers negate identity, but identity is a requirement for EHRs. The table below summarizes how anonymizing technologies fit EHR privacy requirements.

Principles	Applicability
Accountability	No - not within design parameters; anonymizers cannot support audit; cannot monitor controls as controls cannot be implemented if there can be no attribution.
Identifying Purposes	No - not within design parameters
Consent	No - not within design parameters
Limiting Collection	No - not within design parameters
Limiting Use, Disclosure, Retention	No - design is contrary to attribution of action; anonymizers cannot support audit; cannot monitor controls as controls cannot be implemented if there can be no attribution.
Accuracy	No - not within design parameters

Safeguards	No - not within design parameters
Openness	No - not within design parameters
Individual Access	No - not within design parameters
Challenging Compliance	No - not within design parameters

2.2 Platform for Privacy Preferences (P3P)

The Platform for Privacy Preferences (P3P) was developed by the World Wide Web Consortium (WWWC) to define a standard for automating a way for users to exert control on the use of personal information by the web sites that they visit. Participants in P3P development include a variety of vendors and others, including America Online/Netscape, American Express, the Information and Privacy Commissioner of Ontario, Microsoft, Citibank, IBM, NEC, Nokia, and the Privacy Commissioner of Schleswig-Holstein. WWWC expects P3P to be in the form of a standard soon.

P3P is a tool intended to permit e-commerce providers to build services that respect users' privacy rights and preferences, while giving users greater control over their on-line privacy through individualized choices about the relationships they want to have with web-based services. P3P operates in a regulatory and policy context; it does not protect privacy in and of itself. In countries that have privacy laws, such as Canada, P3P can be used to assess privacy statements, allowing them to be collected and analyzed, and then assessed for compliance. P3P has the potential to enhance transparency and accuracy, but P3P does not guarantee that organizations follow their privacy policies.

P3P defines a standard set of practices related to the collection of private information. Web sites define how they intend to handle any data they collect. Individuals define, using multiple-choice questions, how they wish their information to be collected and handled. P3P-enabled browsers can then compare an individual's wishes to the Web-site policy and allow a user to proceed with the link knowing about the differences between their preferences and the site. A P3P Preference Exchange Language (APPEL) is used to encode the user preferences and the site policy and to directly take specific actions.

Users can also use P3P facilities to store data that they frequently exchange with web sites.

New concepts envision P3P as the basis for designing an identity management system, which will allow users to manage their privacy and control their digital identity. This concept is discussed in paragraph 2.4 below.

Assessment of P3P:

P3P was developed to help users to assess how a web site handles their personal information. It can also help organizations develop privacy policies and practices. P3P technology can assist the health sector in developing and managing privacy policies where information is exchanged over the Internet through web portals or sites, including how information is shared among linked services. This approach could ensure consistency.

P3P's major weakness is that it does not provide assurance that an organization complies with its own policies. The technology does not include security features such as access control, identification and authentication. In addition, it is intended for direct interchange between individuals and web sites. P3P offers limited support for the current EHR model, and only if OHIH anticipates that the patient will play a direct role in permitting data to be linked and/or in managing their records. Assessing P3P's ability to support privacy principles is a challenge: P3P addresses policy checking only, and does not include security features. Its usefulness also depends on the patient's role in EHR design. The table below therefore assesses only what a user can know is implemented.

Principles	Applicability
Accountability	No - not part of design parameters
Identifying Purposes	Yes - providing that policy is followed
Consent	Possibly - depending on EHR design: Patients have the choice to provide the information being asked if they agree with the policies; there is still no guarantee that policy is followed
Limiting Collection	Possibly - depending on EHR design: only information that patients consent to have collected, is collected, providing policy is followed and no unseen processes have been implemented to collect additional information.
Limiting Use, Disclosure, Retention	No - not part of design parameters
Accuracy	No - not part of design parameters
Safeguards	No - not part of design parameters
Openness	Yes - if policy is followed; policy content is verified using P3P tools
Individual Access	No - not part of design parameters
Challenging Compliance	No - not part of design parameters

2.3 Infomediaries and Identity Management Systems

A few companies have introduced tools and services designed to help users manage their on-line identities. These information intermediaries - infomediaries - offer tools that allow users to store personal information in a secure location. This information can then be used, through automatic form filling, to restrict the information individuals wish to share to those sites that match their privacy preferences. Some vendors are "incubators" for infomediaries, setting up companies that act as infomediaries. Some appear to be primarily oriented to customer relationship management, although their products feature maintenance and respect of customer consent as information is exchanged. Some have integrated biometrics as part of their solution, and offer electronic wallets or other forms of e-cash.

Some infomediary tools are based on P3P. P3P platforms, when coupled with an anonymous communications network, offer identity management systems. These tools allow users who wish to be known by different names in different contexts to manage their various combinations of identity, roles and personal data. Identity management systems allow the user to decide to whom to give which data, when to act anonymously, when to use a pseudonym, and when to identify or authenticate. Some systems provide certified pseudonyms that can be used when a real identity is required, for example, for a business transaction, for voting in an election, to pre-authorize purchases, to register for warranties, etc. Certificates can be transferred or used as vouchers, with on-line verification and expiry dates where required.

In well-structured infomediaries, only the user/ information owner is able to link their pseudonyms. Data, however, is stored centrally and could be logged and analyzed to gain a detailed picture of user behaviour by the infomediaries themselves. Implementations with this type of data aggregation are potentially privacy-invasive.

Assessment of Infomediaries and Identity Management Systems:

This type of technology combines identity management with anonymizers and P3P techniques to help users of the Internet manage different identities. This technology itself needs to adhere to the privacy principles so that users can monitor the way in which they allow their information to be distributed. These tools implement few of the privacy management requirements that are listed in Table 1 either for the systems they allow pseudonym access or for the personal data they contain.

As for basic anonymizing technology, the objectives of infomediaries and identity management systems are to dissociate an individual from their personal information. This appears to defeat the main purpose of the virtual EHR systems, which is to insure all of an individual's information is readily available to authorized parties.

The authors believe that infomediaries could play a role in EHR systems, although they are not designed to do so. These types of identity databases could be used to link an individual's existing records by keeping track of the various identifiers that are used for one person in different EHR source databases. This would allow the custodian/owners of each health database to manage information in the most efficient way possible for them while at the same time provide that information to other health professionals without undue restrictions. If the infomediary could capture use information, this would allow patients some measure of control on information that has been collected about them, if EHR design permits patients a direct role in the EHR.

Principles	Applicability
Accountability	No - not part of design parameters
Identifying Purposes	Possibly - providing that P3P-like policy is stated and followed
Consent	Possibly - Depending on EHR design: patients have the choice to provide the information being asked under their real identity or using a pseudonym
Limiting Collection	Possibly - providing that P3P-like policy is stated and followed
Limiting Use, Disclosure, Retention	Possibly - depending on EHR design, and if creation of identity databases and multiple identities are permissible; tool needs to capture use information
Accuracy	No - not within design parameters
Safeguards	No - not within design parameters
Openness	Yes - if P3P-like policy followed
Individual Access	Possibly - depending on EHR design and if use information is captured
Challenging Compliance	No - not within design parameters

2.4 Trust Management Systems

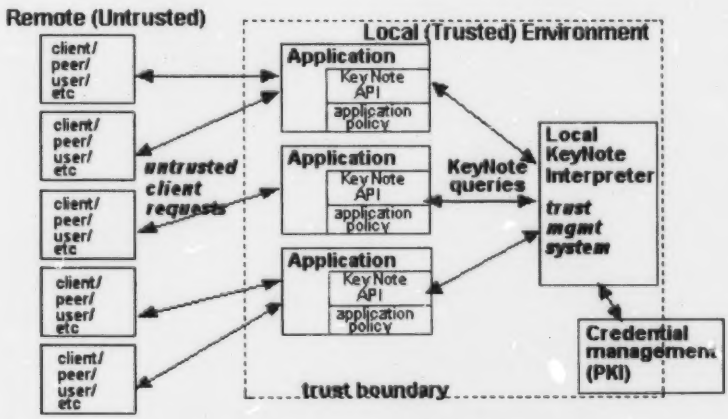
A trust-management system helps applications answer questions of the form, "Does this potentially dangerous operation conform to my security policy?" Typically, the correct answer depends on what the operation is, who is requesting that it be performed, the local security policy, the requester's credentials, and other factors. Trust management systems provide applications with a standard interface for getting answers to such questions, and provide users with a standard language for writing the policies and credentials that control what is allowed and what isn't. There are five components to a trust management system:

- A language for describing actions, which are the operations with security consequences that the system controls;
- A mechanism for identifying principals, which are entities that are authorized to perform actions[5];
- A language for specifying application policies, which govern the actions that principals are authorized to perform;
- A language for specifying credentials, which allow principals to delegate authorization to other principals;
- A compliance checker, which provides a service to applications for determining how an action requested by principals should be handled, given a policy and a set of credentials.

In traditional applications, policies are often "hard-coded" into applications and are difficult to change. In a Trust Management system, policies are written in a standard language that stays the same across different applications, that is defined outside of the application's code and that can be altered by the responsible user whenever needed. An especially powerful concept is the unification of the notion of security policy with that of security credentials. Distributed applications can easily create polices that defer to a remotely managed authority, which can change the policy simply by issuing new credentials (certificates). A policy can become a remotely usable credential simply by being signed.

Using a trust management system for controlling security-critical services frees the application developer from a number of often difficult and subtle design and implementation issues, and allows users to take advantage of a flexible, standard, application-independent language for specifying policy. Before trust management, every application had to provide its own mechanisms for specifying policy, interpreting credentials, and binding user authentication with the authorization to perform "dangerous" operations. Trust management systems, on the other hand, provide an interface that potentially takes care of all of these things. All the application designer has to do is identify the trust management questions in the application and formulate appropriate queries to the trust-management system.

The diagram below, taken from the overview of the "Keynote Trust Management Architecture", illustrates how this technology works:



KeyNote Trust Management Architecture

Assessment of Trust Management Systems:

Trust management unifies the notions of security policy, credentials, access control, and authorization. An application that uses a trust-management system can simply ask the compliance checker whether a requested action should be allowed. These could include the access principles required for the management of private information.

Furthermore, policies and credentials are written in standard languages that are shared by all trust-managed applications; the security configuration mechanism for one application carries exactly the same syntactic and semantic structure as that of another, even when the semantics of the applications themselves are quite different. Trust-management policies are also easy to distribute across networks, helping to avoid the need for application-specific distributed policy configuration mechanisms, access control lists, and certificate parsers and interpreters.[6]

This type of technology seems to offer many of the features that would be needed by EHR systems to help manage who can access and use a person's information. Trust Management, however, adds a layer of complexity to managing private information without necessarily providing the controls the ten privacy principles impose on the collection of information.

Principles	Applicability
Accountability	Yes - Trust rules can be designed to ensure consent, limit use and disclosure, protect other access, and allow individual access. These rules can also be audited, thus providing the accountability defined by privacy. The PKI support for authentication can provide some assurances about the identity of the users and administrators.
Identifying Purposes	Yes - certificates can be created for each purpose
Consent	Yes - can be part of the certificate creation process.
Limiting Collection	Yes - by design (see Identifying Purposes) plus audit
Limiting Use, Disclosure, Retention	Yes - combination of credentials, access management supported by PKI, logging and audit
Accuracy	Yes - Using PKI digital certificates for integrity; collectors cannot modify information unless they are assigned the proper credentials.
Safeguards	Partial - provides access control mechanisms
Openness	No - Only in policy statement; not part of design parameters
Individual Access	Yes - suppliers of information could have the credential to access their information depending on EHR design + users with the appropriate credential can verify accuracy.
Challenging Compliance	No - not part of design parameters

2.5 Smart Cards and Personal Computer Cards

Smart card technology has progressed to the point where the increased capacity for memory and functionality permit the creation of secure solutions for a wide range of situations. Smart cards have been used since the early 1970s for many different types of applications. In their most common form, they contain stored values that are transmitted when the card is inserted into a reader, or for some newer version, when they are in close proximity to devices that receive

radio frequencies. Many smart card implementations include complex crypto logic protocols that allow these devices to be used to protect the confidentiality of the stored information.

Smart cards can be used to store credential information, such as academic qualifications, credit rating and permission to access a room; and produce evidence that the individual holds credentials without the individual having to reveal the personal information that is ordinarily required for verifying credentials. In Europe, smart cards are widely used for processing transactions with retail, telephony and information retrieval applications, particularly for electronic "purses". Personal Computer (PC), Personal Computer Memory Card International Association (PCMCIA), Miniature, SmartMedia, MultiMedia and CompactFlash cards offer different memory capacity and vary in size as well as in compatibility with card and socket services.

Smart cards can store information that defines a person's identity: Using a reader, a person can authenticate to a computer system to retrieve or store information. Such an interface to an access control system or to a Permission Management Infrastructure can be used to allow authorized access to information according to pre-set rules. In addition, they can store records of personal information. Anyone needing access to that information needs to have possession of the card and the authority to read the information it contains. Although the authors have not identified any devices that can do so, Smart Cards with appropriate programming could capture usage and access data. This reporting feature would allow Smart Cards to meet many of the privacy reporting requirements described earlier.

Assessment of Smart Cards and Personal Computer Cards:

Although Smart Card technology has the potential to hold medical records and can help users manage who gains access to those records, most current uses of the technology are limited to storing information that is used to confirm the identity of its holder or to store encryption keys used to encrypt information. Much development work, therefore, remains to be done to apply Smart Card technology to the management of personal information.

Principles	Applicability
Accountability	No - not part of design parameters
Identifying Purposes	No - not part of design parameters
Consent	No - not part of design parameters
Limiting Collection	No - not part of design parameters
Limiting Use, Disclosure, Retention	No - not part of design parameters
Accuracy	Partial - if card contains digital signature
Safeguards	Partial - provides high assurance verification of identity
Openness	No - not part of design parameters
Individual Access	No - not part of design parameters unless EHR design requires token for patient access
Challenging Compliance	No - not part of design parameters

2.6 Biometrics and Biometric Encryption

The progress of biometrics[7] using fingerprints, voiceprints or retinal scans, promises to deliver a high degree assurance for processes that validate the identity of individuals. A biometric device authenticates an individual and verifies eligibility to access a service or specific information. Biometric verification replaces a password or PIN, and offers the benefit of stronger authentication than a password or a PIN to counter identity fraud. Control of the stored digital

biometric representations, and of their encryption keys where cryptography is used, is the weak link in this model, and information from a variety of sources can still be linked to or associated with the biometric template, thereby permitting third parties to have access to detailed, complete personal profiles.

Encryption based on a biometric key can be used to anonymize information in a database by separating an individual's identity from the personal information. The link between the identity and the information is a pointer that is encoded by the individual's fingerprint pattern, for example, or other biometric representation. The individual now controls that personal information.

Some biometric technology is not as stable as required for widespread large-scale use. Fingerprint and retina patterns can change according to conditions or to alterations from accidents and are thus are not reliable. Retinal scans continue to offer the most promising solutions, although most Canadians resist them as invasive. Voice recognition technology is also making significant progress and has been implemented in many smaller scale applications. Biometric technology is relatively expensive.

Assessment of Biometrics and Biometric Encryption

Biometrics and biometric encryption offer possibilities for strong identification and authentication when used in combination with smart card or personal computer cards, and possibly with PKI and/or trust management systems. Biometrics offers the strongest possible identification and authentication for individuals who are authorized to enter or retrieve data from an EHR. In the case of health care organizations, such as hospitals, this level of granularity may not be warranted, unless it is the patient who uses a card to permit data to be entered or retrieved. Many individuals find biometrics to be invasive, and resist using the technology; others assess biometrics as privacy neutral.

Using biometrics as part of an EHR system requires implementers to pay attention to how the biometric record is stored for back-up purposes. In addition, proper registration of individuals is a major challenge, especially if biometrics devices are to be used in large numbers.

Principles	**Applicability**
Accountability	No - not part of design parameters
Identifying Purposes	No - not part of design parameters
Consent	No - not part of design parameters
Limiting Collection	No - not part of design parameters
Limiting Use, Disclosure, Retention	No - not part of design parameters
Accuracy	Partial - if card contains digital signature
Safeguards	Partial - provides high assurance authentication of identity
Openness	No - not part of design parameters
Individual Access	No - not part of design parameters unless the patient controls the electronic health record
Challenging Compliance	No - not part of design parameters

↑

2.7 Public Key Infrastructure and Public Key Certificates

Public Key Certificates (certificates) are part of a Public Key Infrastructure (PKI), and normally require that the identity of an individual is validated to varying degrees of rigour, and bound to

the digital signature and confidentiality certificates issued by a Certification Authority (CA). The individual's public key is kept in a directory, which is accessible to anyone with a certificate recognized by the directory. PKIs offer a range of security services, including encryption, digital signature, non-repudiation, and identification and authentication. New versions of PKI offer a number of features, including permissions management.

Public key infrastructures support the use of applications that encrypt data and that use digital signatures. Public key infrastructures are based on principles associated with public key cryptography. Public key cryptography encrypts information by using two mathematically related keys: one is kept private; the other is made public. The private key cannot be determined from the public key. An individual who wants, for example, to send a message uses the public key of the recipient to encrypt the message. The recipient uses his or her private key to decrypt the message. The sender therefore knows that only the intended recipient can read the message.

Public key cryptography can also be used to create digital signatures. A digital signature uses a mathematical function to produce a value that depends on the content(s) of a message. This value is then attached to the message and encrypted using the sender's private key. The recipient of the message then decrypts the digital signature using the sender's public key and recreates the value that was attached to the message using the same mathematical function as the sender. If the digital signature can be decrypted and the attached values are identical, then the recipient is assured of both the sender's identity and the integrity of the message. Because the digital signature of a message depends on the private key used to produce it, the sender's ability to repudiate the message is reduced.

Keys are managed by a Certification Authority, which may be a third party trusted to associate a public and private key pair with a specific individual or entity, called a subscriber. It manages the issuance and revocation of certificates, and maintains lists of certificates that have been revoked. Digital certificates, which are digitally signed by the Certification Authority, contain the public key and serves as evidence that the individual identified in the certificate holds the corresponding private key. Two or more Certification Authorities can be linked together by cross-certification to provide mutual recognition of the certificates issued by different organizations.

There are a number of privacy-invasive features in PKI, most notably the posting of public keys on a directory accessible to all those holding keys issued by a Certification Authority or by Certification Authorities that are cross certified. This technology can potentially be designed to support privacy by using pseudonyms or some other method to disguise the identity of the certificate holder. Registration procedures still bind the real identity of the certificate holder to the certificate.

Assessment of Public Key Infrastructure

PKI is a relatively mature technology that, when used in combination with other technologies, offers considerable promise for EHRs. Although PKIs require a major effort to implement, including considerable attention to governance, policy and practices, they offer a number of features that will help EHRs support privacy principles: identification and authentication, non-repudiation, policy management and standards, and confidentiality. A permissions management infrastructure can be used in conjunction with PKI.

Successful implementation of a PKI requires strong policy management within an organization, the Certification Authority and across cross-certified organizations. PKIs have built-in audit requirements, and standards. PKI also requires that subscribers agree to protect their keys by signing a formal agreement that could also serve as the formal consent for collection and use of at least some personal information. PKI also offers the possibility of deploying an infrastructure that permits devices rather than individuals to access, enter or change data.

The close association between the certificate issued by a PKI and the identity of its recipient, the subscriber, is usually viewed as in conflict with privacy principles. If patients are subscribers, then directories pose a potential privacy violation unless an identifier or other method is used. Treasury Board Secretariat is exploring ways to address this problem. Seamless ways to register

subscribers and issue certificates are also required to make this model scalable.

In spite of its maturity, PKIs are tools for verifying the identity of individuals before they are allowed to access specific in formation or processing resources. By itself, this technology does not provide for the privacy principles and requirements outlined above. PKI, however, identifies subscribers with high level of assurance. Application interfaces that link these identities with EHR records are needed to ensure that personal data does not end up in unauthorized hands.

Assessing PKI's ability to meet privacy requirements is difficult, as PKI relies heavily on policy and policy management as well as safeguards. Policy and audit, along with policy management, are intended as checks and balances; policy must be designed as privacy-compliant, and audits must be public. The policy burden that accompanies PKI is further complicated if a permissions management infrastructure is used, although permissions management can help PKI meet privacy requirements. The assessment below indicates where policy can be audited for compliance to meet policy requirements; where EHR design and the patient's role in EHR could determine whether PKI meets requirements; and where a permissions management infrastructure will help PKI to support privacy requirements.

Principles	**Applicability**
Accountability	Yes - audit and policy management
Identifying Purposes	Yes - Certificate Policies and Certificate Practice Statement can state purposes and set standards for adherence to stated purposes; audit
Consent	Possibly - if patients issued certificates and subscriber agreement includes consent to what is stated in Certificate Policies
Limiting Collection	Possibly - if permissions management infrastructure used
Limiting Use, Disclosure, Retention	Possibly - if permissions management infrastructure used, and Certificate Policies state use, disclosure, retention, and audit can track Directory problem must be addressed (see text above)
Accuracy	Partly - through preservation of digitally signed records
Safeguards	Yes - provides verification of identity, encryption for confidentiality and digital signatures for accountability (non-repudiation)
Openness	Yes - Certificate Policies, which need to be subject to audit and audit results must be published
Individual Access	Possibly - if patients have access permissions in a permissions management infrastructure
Challenging Compliance	No - not part of design parameters

3 Applicability of Privacy Enhancing Technologies for Meeting

Privacy Requirements

Summary of Findings

This section summarizes privacy requirements as developed in Section 1, listed according to the ten privacy principles, and indicates the technologies that potentially satisfy each requirement. This table includes methods, other than design, that could or do satisfy requirements. Where a PET's design satisfies a requirement the authors have noted this in bold font.

Requirements	Applicable PETs[8]
3.1 Accountability	
1. Permit organization's accountable person to manage personal information use, disclosure etc.	P3P - If policy is followed and audit possible, can have policy management across jurisdictions and systems **PKI - audit and policy management** **Trust Management Systems - Design with PKI support for identification and authentication; rules can be audited**
2. Verify adherence to principles e.g. audit trail	**PKI - digital signatures (non-repudiation) within permissions management infrastructure; and audit** **Trust Management Systems - Design: Audit**
3. Collect/monitor status of controls used to manage other principles	**PKI - Certificate Policy audit requirements and audit of permissions management infrastructure** **TRUST MANAGEMENT SYSTEMS - DESIGN: AUDIT**
4. Report the status of controls and assist in managing privacy issues	**PKI - audit and policy management** **TRUST MANAGEMENT SYSTEMS - DESIGN: AUDIT**
3.2 Identifying Purposes	
1. Document purposes and track changes to purposes	P3P if policy followed Informediaries - if P3P-like policy followed **PKI - Certificate Policy and policy management; audit** **TRUST MANAGEMENT SYSTEMS - DESIGN: CREATE DIFFERENT CERTIFICATES FOR EACH IDENTIFYING PURPOSE**
2. SUPPORT ACCOUNTABLE PERSON	**PKI - CREATION OF POLICY MANAGEMENT AUTHORITY AND PUBLICATION OF CERTIFICATE POLICY; AUDIT** **Trust Management - Design: audit certificate use**
3. DOCUMENT WHEN AND HOW INFORMATION OWNER NOTIFIED OF PURPOSE AND CHANGES TO	P3P AND INFOMEDIARIES - IF POLICY FOLLOWED **PKI - CERTIFICATE POLICY;**

PURPOSES	**POSSIBLY THROUGH SUBSCRIBER AGREEMENT IF PATIENT IS A SUBSCRIBER; AUDIT**
3.3 Consent	
1. Document history of consent given	P3P - depends on EHR design and whether policy is followed; Infomediaries - depends on EHR design PKI - possibly through subscriber agreement if patient is subscriber **Trust Management - part of certificate creation** Biometrics/Biometric Encryption - Individual's use of biometric may be tacit consent; use could be logged Smart Card -as for biometrics
2. Audit or review consent database	PKI - maintaining subscriber agreements where patients are subscribers (manual) **Trust Management -Verification of credentials database**
3.4 Limiting Collection	
1. Document how each item supports purpose	P3P and Infomediaries - if policy implemented PKI - Possibly - Certificate Policy, Subscriber agreements where patient is subscriber, permissions management infrastructure **Trust Management - See Identifying Purposes (3.2)**
2. Document how collection made	P3P and Infomediaries - if policy implemented PKI - Possibly - Certificate Policy, Registration model, Subscriber agreement where patient is subscriber; audit **Trust management - See Identifying Purposes**
3. Audit or review collection	**PKI - Certificate Policy audit requirements** **Trust Management - See Identifying Purposes**
4. Capture explanation of why data item being collected	PKI - Possibly through Certificate Policy and subscriber agreements where patient is subscriber **Trust Management - See Identifying Purposes**
5. Capture explanation of how collection being done	PKI - Certificate Policy and subscriber agreements where patient is subscriber **Trust Management - See Identifying Purposes**
6. Collect information according to defined rules and definitions	P3P and Infomediaries - if policy implemented PKI - Certificate Policy, registration model, subscriber agreements where

	patient is subscriber **Trust Management - See Identifying Purposes** Biometric - if patient has control over HER
3.5 Limiting Use, Disclosure, and Retention	
Use	
1. Document information use(s)	P3P and Infomediaries - if policy implemented PKI - possibly through permissions management, Certificate Policy **Trust Management - through credentials**
2. Document authorized access to the information; define the roles	P3P and Infomediaries - if policy implemented PKI - possibly through permissions management **Trust Management - through credentials**
3. Manage access based on authorization	P3P and Infomediaries - if policy implemented PKI - possibly through permissions management infrastructure **Trust Management - through credentials**
4. Audit access and use	PKI: possibly through permissions management, Certificate Policy audit requirement, log intrusions **Trust Management: through credentials, audit compliance checker**
5. Capture who can obtain access	P3P and Infomediaries - if policy implemented PKI - possibly through permissions management infrastructure **Trust Management - through credentials**
6. Permit authorized access and disallow other access	**PKI - Identification and Authentication;** possibly through permissions management infrastructure **Trust Management - through credentials + PKI for access controls and audit**
7. Capture / log access requests	**PKI - database access logs or intrusion logs** **Trust Management - PKI database access logs or intrusion logs**
8. Report access requests outside of defined authorizations	**PKI - Certificate Policy, Certificate Practice Statement, safeguards, intrusion alarms and logs** **Trust Management - PKI database access logs**
Disclosure	

1. Deny use/ access/ receipt based on authorizations/ permissions and exclusions	P3P and Infomediaries - if policy implemented PKI - Possibly through built-in Identification and Authentication combined with permissions management infrastructure **Trust Management - through credentials and PKI identification and authorization controls** Biometric Encryption - credentials for those authorized or patient control through biometrics Smart Card if patient controls HER
2. Audit access/receipt	**PKI - identification and authorization controls** **Trust Management - PKI identification and authorization controls**
3. Capture exclusions in authorization/ permissions rules	P3P and Infomediaries - if policy implemented **PKI - through permissions management and identification and authorization controls** **Trust Management - through credentials and PKI identification and authorization controls**
4. Report access/ receipt by excluded roles	**PKI - through permissions management and identification and authorization controls; and log database access** **Trust Management - through credentials and PKI identification and authorization controls; and log database access**
5. Track authorized disclosures/receipts	**PKI and Trust Management - log database access**
Retention	
1. Document rules for retention	P3P and Infomediaries - if policy implemented PKI - possibly through Certificate Policy, Certificate Practice Statement Trust Management - policy
2. Document how information is to be disposed of	P3P and Infomediaries - if policy implemented PKI - possibly through Certificate Policy, Certificate Practice Statement Trust Management - policy
3. Audit disposal of all information in a collection	PKI - Certificate Policy audit requirements Trust Management - audit requirements
4. Audit destruction and verify	PKI - Certificate Policy, Certificate Practice Statement Trust Management - through PKI as above
5. Capture, hold, manage records	PKI - Certificate Policy, Certificate

for long retention periods	Practice Statement, notary services Trust Management - through PKI as above
6. Inventory all copies (backups, all subsets, all media)	PKI - Certificate Policy, Certificate Practice Statement Trust Management - through PKI as above
7. Document/ capture all steps in collection's life cycle	PKI - Certificate Policy, Certificate Practice Statement Trust Management - through PKI as above
3.6 Accuracy	
Defined accuracy and maintenance checks	Smart Cards and Biometrics: if digital signature used, and uses logged PKI - partly through digitally signed records **Trust Management - collectors cannot modify information unless they are assigned the proper credentials + digital signature for integrity**
Integrity designed into collection and retention mechanisms, across collections	Smart cards and Biometrics: if digital signature used PKI - partly through digital signature **Trust Management - collectors cannot modify information unless they are assigned the proper credentials + digital signature for integrity**
See Individual Access (3.9) and ability to correct information	
3.7 Safeguards	
1. Information protection due diligence	Smart Cards and Biometrics - if cards can encrypt, digitally sign; use identification and authentication **PKI - encryption, digital signature - appropriate assurance level** **Trust Management - through PKI**
2. Accepted security practices (standards)	Smart Cards and Biometrics - if cards can encrypt, digitally sign; use identification and authentication **PKI - Certificate Practice Statement for encryption, digital signature, physical security, subscriber agreements,; cross-certification agreements; technical, physical and personnel security** **Trust Management - provides access control mechanisms**
3. Confidentiality and integrity objectives considered high	Smart Cards and Biometrics - if cards can encrypt, digitally sign; use identification and authentication **PKI - Design: encryption, digital signature, non-repudiation, back-up** Trust Management - use PKI for safeguards

4. Right to access very limited	Smart Cards and Biometrics -use identification and authentication **PKI - identification and authentication, registration model**; possibly through permissions management **Trust Management - credentials Biometrics, Biometric Encryption for stronger access control** where required
5. Safeguards selection based on requirements	Smart Cards and Biometrics - if cards can encrypt, digitally sign; use identification and authentication - can augment other safeguards **PKI - Safeguards, based on selection of appropriate assurance level** Trust Management - through PKI
6. Approach can be HAZOP, ISO17799, Cobit or other recognized standard	As above
7. Specific data protection tools justified to meet objectives	**PKI - selection of appropriate assurance level** Trust Management - through PKI
8. For long-lived records, must allow for retrieval across generations of technology: software and hardware can become part of the record so that the record can be read throughout its life	PKI - notary services can help maintain document integrity Trust Management - possibly through notary services
3.8 Openness	
1. Mechanism(s) for policy accessibility	**P3P and Infomediaries - publication of policy; accessible for policy matching across organizations sharing information** **PKI - Publication of Certificate Policy with published audits**
2. Mechanisms for individual to receive/ access status of information including use, disclosure (includes who has access to the information), disposal	P3P and Infomediaries - policy checking only Trust Management and PKI - See Individual Access (3.9)
3. Mechanisms to track collection, use, disclosure, consents, disposal	**PKI - audit of permissions management, intrusion logs, log access requests to database**
3.9 Individual Access	
1. Permit information owner access; block exceptions (identification and authentication)	Infomediaries - depending on EHR design and if use information is captured **Tokens: Biometrics, Biometric Encryption - patient Smart Card/ PC Card for patient access where patient controls EHR (see Trust Management below)** PKI - partially through identification and authentication where patient is a

	subscriber; possible requirement for token **Trust Management - suppliers of information could have credential to access their information depending on EHR design.**
2. Record who requests, how, when	**PKI - log intrusions; log database access requests** **Trust Management - as for PKI**
3. Reliable change management process to record requests, action them, track changes and confirm them to information owner	PKI - allow for policy changes through policy management authority and public posting of Certificate Policy Trust Management - as for PKI
4. Mechanism for propagating the change across all copies of collections that include the individual's information	PKI - changes to permissions management, potential to re-issue certificates **Trust Management - Design**
3.10 Compliance	
1. Audit compliance challenges and responses	

4 Conclusions and Recommendations

4.1 General

The design of current privacy technologies does not meet the functional requirements that are implied by privacy codes and legislation. None of the technologies surveyed provides appropriate tools that allow privacy managers to answer the basic questions about the private information they keep: What is it used for, Who has access, When was the last access, Is the collection safe and sound, and so on. Not surprisingly, no PET addresses all requirements, and no tools specifically address compliance challenges, partly because administering challenges will come outside of the EHR. As noted in the introduction, the authors acknowledge that technology alone is capable of addressing few requirements. For some, however, such as anonymizing technologies and Platform for Privacy Preferences, there is no built-in technology to support policy. Smart Cards and Biometrics can address few requirements by themselves, but are capable of augmenting promising PETs.

Many of the tools identified limit their functionality to hiding the identity of their users or to permitting the creation and management of several pseudo-identities that serve to hide the real individual. The authors believe this is incompatible with the requirement that EHR records be clearly linked to an individual for purposes of integrity and accountability, and therefore conclude that anonymizers, Platform for Privacy Preferences and Infomediaries are unsuitable for EHRs.

Other technologies, such as PKI, meet privacy requirements primarily through the application of policy and subscriber agreements. This technology will require attention to policy, procedure and processes, and will have to include governance, policy management, and compliance auditing at a minimum. Interoperability will also be a technology and budget issue. Technology that relies on voluntary adherence to privacy policy also needs some form of substantiation that policies are being followed. The tools surveyed provide neither the policies nor the assurance that they cannot be circumvented. For trust management systems, policy is propagated across applications, and technology, such as PKI, is available to enforce permissions management and other policy requirements. Those entrusted with designing EHRs and EHR systems must therefore get the policy right.

The authors thus conclude that although many tools claim to support privacy, this support is

usually limited to a very narrow objective that in many creates a governance conflict within EHRs. None of the tools provide the support that a privacy administrator will require to monitor adequately whether or not an organization's application adheres to the privacy principles.

Using the privacy principles, the authors identified a number of requirements that applications need to add to their traditional business specifications. Many of the requirements are reflected in the table in Section 3. Only those applications that factor in privacy during their development have the potential to satisfy all privacy needs. The six categories of privacy technologies from Section 2 are further grouped below, according to the authors' assessment of their potential for supporting privacy requirements.

4.2 Unsuitable PETs

Some PETs are not suitable for EHRs. Our recommendation is to not use these tools in the health context now.

Anonymizers:

Anonymizing technology, by design, does not permit attribution of actions, such as entering or retrieving data. Policy-compliant EHRs will require that at least some actions will need to be attributed to an individual or organization, that is, it is not possible to impose accountability. In addition, anonymizers provide no other protection for safeguarding the availability, confidentiality and integrity of records, transactions and other aspects of EHRs. While safeguards could be added, the inability to impose accountability is considered serious enough to assess this technology as having no potential for use in EHRs, either now or in the future.

Platform for Privacy Preferences (P3P)

While P3P assists organizations to develop privacy-compliant policy and practices, it provides no assurance to the community of EHR users and patients regarding compliance. As with anonymizers, P3P does not safeguard information through access control, encryption and other standard security safeguards. These features could be added, but the uncertainty of policy application is a serious limitation on true openness, accountability, and limitations on use, disclosure and retention. P3P, therefore, offers little or no promise for EHRs.

Infomediaries and Identity Management Systems

The combination of identity management and infomediaries does not permit an EHR system based on this technology to impose accountability. In addition, those that are P3P-based, the majority, will not be able to provide compliance assurance. Infomediaries and Identity Management Systems have some limited potential for use in EHRs, depending on design, and could be used to manage multiple identities where these are permitted.

4.3 Useful PETs

Some PETs have useful features that could be incorporated with other technology in an EHR framework:

Smart Cards and Personal Computer Cards

These technologies are capable of strengthening access control through strong identification and authentication, and could be used to support permissions management. This technology, similar in use to credit and debit cards, should be examined for its potential, given its wider acceptance among less sophisticated users.

Biometrics

This technology, when coupled with smart cards, could provide additional access controls and permissions management. Storage of biometric information will have to be handled very carefully, and registration of individuals in large-scale deployments poses a major challenge. This technology could be effective if EHRs need to incorporate some degree of direct patient access to patient information. Some forms of biometrics are, at present, less acceptable than others.

↑

4.4 Promising PETs

Two types of technologies merit detailed examination: Trust Management Systems and Public Key Infrastructures.

Trust Management Systems

Trust Management Systems offer a number of attractive features, including permissions management and policy compliance enforcement. This technology also permits development of an EHR system that is tailored to meet the unique requirements of the health community through use of application-independent language and simple interfaces. The unification of policy and credentials permits accountability, access control and permission management. One of the most attractive features of Trust Management is that IT security and privacy policy compliance is application-independent, unlike PKI (see below). This technology should be explored in more detail to further identify its potential for EHRs, and to identify potential weaknesses.

Public Key Infrastructures (PKIs)

Public Key Infrastructures are primarily a tool to validate the identity of individuals who require access to specific resources: files, e-mails, authorizations, etc. A valid identity then provides for an application to verify accountability for actions taken during the collection and processing of private information. This technology offers the advantage of being fairly well understood, and it is being implemented in a number of jurisdictions, including the federal government and a number of provinces. The information about individuals held in a PKI directory is itself a privacy concern, especially given the trend to provide more and more data about certificates and their holders.

PKIs require careful attention to governance and policy management, and rely on subscribers to maintain the confidentiality of their private keys. A number of new tools make registration and certificate issuance more straightforward. The number of applications that support PKI is growing, but it is probable that applications will need to be coded to accept encryption and digital signatures as well as permissions management and other tools. This technology merits further exploration to identify its potential for EHRs, and to determine whether certain privacy-unfriendly features can be neutralized or re-engineered.

Combined Solution

The most promising technology combination for EHRs appears to be a combination of Trust Management and PKI, possibly enhanced with smart cards and biometrics. PKI can supply many of the required safeguards such as strong encryption for confidentiality and digital signatures, and Trust Management design can propagate the certificates that are used by the access control components to enforce privacy-supporting practices. Some of the internal management tools that have been built into these types of systems can actually provide information about the privacy practices implemented as part of an application.

↑

4.5 Recommendations

Detailed recommendations are not possible at this stage in the assessment of privacy technologies. The following recommendations in general are to follow those technologies that promise to address privacy requirements that can support the correct policy, and to reject those that cannot:

Recommendation 1: OHIH should explore Trust Management Systems and Public Key Infrastructure in some detail.
Recommendation 2: OHIH should consider the use of smart cards and possibly biometrics to enhance privacy where stronger limitations on access and other actions are required.
Recommendation 3: Where multiple identities are permitted, OHIH should consider the potential of using infomediaries.
Recommendation 4: The activities above should proceed in parallel with the development of the EHR concept so that technology and requirements can be developed together.

---

[1] Most organizations envision limits to patient access, such as requiring a health provider's guidance for access to specific information.

[2] The OECD adopted eight privacy principles. The Canadian Standards Association and Canadian legislation (the *Personal Information Protection and Electronic Documents Act*) identify ten. The U.K., the EU, New Zealand, Australian and Hong Kong legislation are similar. There is no national privacy legislation in the U.S.A. The American *Health Insurance Portability and Accountability Act* addresses privacy more as a function of confidentiality.

[3] Used by the petrochemical industry to meet environmental guidelines: identifies potential hazards for each component in a process and identifies how to manage each hazard.

[4] Privacy technologies are commonly referred to as Privacy Enhancing Technologies (PETs), and the authors use this more common term from vendor literature and privacy web sites.

[5] A principal can be a physical entity, a process in an operating system, a public key, or any other convenient abstraction.

[6] Further information is available at http://www.cis.upenn.edu/~keynote/Papers/rfc2704.txt

[7] Authentication can be one, two or three factor: something a person knows, something they have or something they are. Biometrics addresses the something that they are, e.g. a fingerprint, voice pattern, retinal scan. The standard biometric model matches a physiological or behavioural characteristic of a person to an established record of that characteristic. More sophisticated biometric technology uses a mathematical representation of a physical characteristic, such as a person's retina, and matches it by taking a digital sample of the biometric credential, the retina. Replay attacks are almost impossible, as the digital sampling should not be the same two successive times; a system can be programmed to reject the second or third consecutive identical reading.

[8] For each applicable PET, the table notes the relevant feature, whether by design or other method such as policy, audit, use of another infrastructure, or other method that satisfies the requirement. Please note that where non-design methods have potential or partially satisfy a requirement the table may appear to contradict the tables in Section 2, where only design was normally commented on.

↑

Annex A: Bibliography

General

The following web sites have good general information about privacy, and links to sites with more specific information. They are primarily U.S. sites that were established for privacy advocacy:

http://www.infosyssec.com/infosyssec/anon1.htm

http://www.epic.org/
http://www.privacyinternational.org/
http://www.privacyrights.org/

A Canadian site primarily for access to Canadian law: http://www.acjnet.org/security.cfm
Industry Canada's e-commerce web site: http://e-com.ic.gc.ca/english/index.html.

The OECD site: http://www.oecd.org/dsti/sti/it/secur/.

Anonymizing Technology

See the FAQ at www.w3.org/Security/Faq/wwwsf7.html.

A good general site is www.anonymizer.com.

Roger Clarke's site has interesting articles and references regarding privacy enhancing technologies and "privacy sympathetic technologies" at
www.anu.edu.au/people/Roger Clarke/DV/PEPST.html.

A list of members of the Information Technology Industry Council, and a good paper about Anonymyzing Technology is available at the ITIC web site: *http://www.itic.org*. The article is copied at Annex B.

http://www.wired.com/wired/archive/4.05/anonymizing_pr.html
http://www.cs.du.edu/~dm/login.html
http://www.zdnet.com/zdnn/stories/news/0,4586,2682476,00.html
http://www.usenix.com/publications/login/1998-5/martin.html
http://www.research.att.com/~lorrie/pubs/networker-privacy.html
http://www.webveil.com/
http://www.wired.com/wired/archive/4.05/anonymizing.html
http://www.hicss.org/HICSS_35/hcmini.htm
http://www.securityoutpost.com/
http://www.ihtml.com/tech/internet.htm
http://mixtersecurity.tripod.com/protecting.html
http://www.sciam.com/2000/1000issue/1000techbus2.html
http://www.ntk.net/
http://www.witsa.org/news/00aug.htm
http://www-swiss.ai.mit.edu/~bianca/swiss_html/users/pmitros/privacy-proto.html
http://anon.efga.org/WebProxies
http://grc.com/downloaders.htm
http://www.lucent.com/press/0697/970610.bla.html
http://www.softouch.on.ca/rc/cookies.htm
http://www.blj8.com/Privacy/index.html
http://www.it.kth.se/~aep
http://www.eros-os.org/~majordomo/e-lang/0363.html
http://www5.zdnet.com/pcmag/stories/opinions/

Platform for Privacy Preferences

The most complete site is the official site for P3P at http://www.w3.org/P3P/.

http://www.cpsr.org/program/privacy/p3p-faq.html
http://www.kcoyle.net/p3p.html
http://www.w3c.org/P3P
http://www.epic.org/reports/prettypoorprivacy.html
http://www.cdt.org/privacy/pet/p3pprivacy.shtml
http://www.research.att.com/projects/p3p/
http://p3ptestbed-1.w3.org/

http://www.wired.com/news/news/story/13242.html
http://www.zdnet.com/zdnn/stories/news/0,4586,2598004,00.html
http://cobra.law.miami.edu/~jb0437/paper.html
http://www.wired.com/news/news/story/12425.html
http://www.wired.com/news/news/technology/story/13242.html
http://www.builder.com/Authoring/P3P/?tag=st.bl.3884.dir1.7584
http://www.uni-siegen.de/security/datenschutz/p3p.html
http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html
http://www.itrain.org/itinfo/2000/it000711a.html
http://www.zdnet.com/zdnn/stories/news/0,4586,2591856,00.html
http://www.w3.org/P3P/nutshell.html

Infomediaries and Identity Management Systems

The one page article, "Infomediaries and negotiated privacy techniques," by Dr. Alexander Dix, Commissioner for Data Protection and Access to Information for the state of Brandenburg, Germany at *www.uni-siegen.de/security/datenschutz/p3p.html*, is a quick overview of infomediaries and P3P and privacy issues, with recommended links for further reading. It is copied to Annex D.

http://www.consciousbuyer.com/
http://www.epsltd.com/Infomediariesmain.htm
http://www.wired.com/news/news/story/18678.html
http://www.eff.org/bayff/20010319_bayff_announce.html
http://sunsite.icm.edu.pl/sunworldonline/swol-07-1999/swol-07-bookshelf.html
http://www.wired.com/news/news/story/18217.html
http://www.thestandard.net/article/display/0,1151,17328,00.html
http://simap.eu.int/EN/pub/docs/ernst/tsld022.htm
http://www.e-commercebc.net/ic_cap_1k.html
http://www.mikealix.com/tb000913.htm
http://www.canada-ecommerce.com/ic_cap_1k.html
http://www.cyberspaceattorney.com/ezine/privacy.htm
http://www.politechbot.com/p-01079.html
http://www.gladwell.com/1999_10_04_a_sleeper.htm
http://www.cfp2000.org/news/student_reports/infomed-muller.html
http://www.junkbusters.com/ht/en/cfp.html
http://simap.eu.int/EN/pub/docs/ernst/sld022.htm

Trust Management Systems

A complete description of the KeyNote Trust Management System: M. Blaze et al, "The KeyNote Trust-Management System Version 2, September 1999, at *crypto.com/trustmgt/kn.html*.

http://www.thethirdpower.com/index.html
http://citeseer.nj.nec.com/context/313424/23045
http://www.crypto.com/trustmgt/kn.html
http://citeseer.nj.nec.com/chu-referee.html
http://www.senate.gov/~scia/hearings/730cobel.htm
http://www.cs.caltech.edu/~adam/papers/www/trust-management.html
http://www.w3.org/TR/REC-DSig-label/
http://link.springer.de/link/service/series/0558/bibs/1740/17400001.htm
http://firstmonday.dk/issues/issue3_6/khare/index.html
http://www.star-lab.com/new.html

Smart Card Technology

A good general explanation of smart card technology is available at smartex.com/smartcards_guide.html. For PC cards, see Bill Lempesis, "The Future of Smart Card Technology, March 1997, at www.smartcardcentral.com

http://www.scia.org
http://www.smartcard.co.uk/
http://www.mac-gray.com/
http://www.smartex.com/
http://www3.goto.com/d/sr/
http://www.fusioncard.com/
http://www.microsoft.com/windowsce/smartcard/
http://www.securenet.com.au/
http://www.tricomcard.com/
http://smart.gov/
http://www.gemplus.com/
http://www.smartcardlaundry.com/smart_cards.htm
http://www.cyberis.fr
http://members.aol.com/pjsmart
http://www.publicard.com
http://www.roaster.com/news/jul97/0728/119.html
http://www.divdyn.com/
http://www.intellect.com.au/
http://www.smartcardforum.asn.au/smartcard.htm
http://www.smartcardhelp.co.uk/
http://www.inlucid.com
http://www.smartcardcentral.com/
http://www.globalplatform.org/
http://www.lifestreamtech.com/
http://www.precis-scs.com/
http://www.tatungtel.com/main1.html
http://www.magcard.com
http://www.sfgate.com/
http://www.macgray.com/
http://www.smartdev.demon.co.uk
http://www.cs.franklin.edu/Faculty/Giuliani/mba682/~mwalter
http://smartcard.a-card.com/index.html
http://www.labcal.com/smartsign.php3
http://www.smartcardclub.co.uk/

Biometrics

Tomko, Dr. George, "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy? Privacy Laws & Business, 9th Privacy Commissioners' Data Protection Authorities Workshop, 15 September 1998; See http://www.aliconferences.com/conferences/biometrics.htm.

For a list of biometric developers and integrators, see biodigest.com.
The U.S. Government site for biometrics is biometrics.org

The Biometric Consortium
www.biometrics.org
U.S. government group focusing on biometric research. Site includes a useful introduction to biometric technologies, uses, and standards.

Biometric Encryption
www.emory.edu/BUSINESS/et/biometric/
Encyclopedia-like discussions of processes, purposes, and implementations of biometric technology.

1998 Glossary of Biometric Terms
www.afb.org.uk/glossuk1.html
Extensive list of terms commonly used in biometrics.

The Biometric Digest

webusers.anet-stl.com/~wrogers/biometrics/
Monthly publication providing biometric product news. Excellent page of hyperlinks to many biometric vendors.

The International Biometric Society

www.tibs.org
Academic society dedicated to exploring the mathematical and statistical aspects of biology.

The BioAPI Consortium
www.bioapi.org
Group formed to develop a standard API for biometric implementation. Discusses biometrics' market penetration and attempts to expand it.

Connecticut's Biometric Imaging Project
www.dss.state.ct.us/digital.htm
The state's Department of Social Services is implementing biometrics into its service-providing processes--a possible model for future large-scale implementations.

http://biometrics.netfirms.com
http://biometrics.cse.msu.edu
http://www.precisebiometrics.com/
http://www.biom.cornell.edu/
http://homepage.ntlworld.com/avanti/
http://stat.tamu.edu/Biometrics/
http://www.zdnet.com/complife/buz/9803/biometricid-6.html
http://www.infosyssec.net/infosyssec/biomet1.htm
http://www.afb.org.uk/
http://www.biometrics.co.za/
http://www.DataCaptureBiz.com/index.asp?page=SRhome.asp&OldDate=2/01/2001
http://www.banking.com/aba/cover_0197.htm
http://www.biometrics-scan.com/
http://www.iosoftware.com/about/employment.htm
http://mason.gmu.edu/~kwong/cs103/index.htm
http://www3.goto.com/d/sr/
http://www.digitalbiometrics.com/
http://www.appliedbiometrics.net/
http://www.biometricgroup.com/a_bio1/technology/research_a_technology.htm
http://www.livegrip.com/
http://www.egroups.com/group/biometrics/
http://www.biometricpartners.com/
http://www.iris-scan.com/
http://www.tibs.org/
http://www.biometricgroup.com/

Public Key Infrastructure

For information about Public Key Infrastructure in the Government of Canada, visit the Treasury Board Secretariat's PKI web site at http://www.cio-dpi.gc.ca/pki-icp/index_e.asp. The site includes FAQs, an overview of PKI, PKI policies and guidelines, and cross-certification information. For federal institutions, this site is the authoritative site about PKI. See also Annex H, Examples of Public Key Infrastructure, and the information from the PKI page (www.pki-page.org/). The IETF page includes information about international standards for PKI (www.ietf.org/).

http://www.ietf.org/html.charters/pkix-charter.html
http://verisign.netscape.com/security/pki/
http://www.itsi.disa.mil/pki/
http://oscar.dstc.qut.edu.au/

http://www.cert.dfn.de/eng/team/ske/pem-dok.html
http://www.certicom.com/
http://www.cse.dnd.ca/cse/english/gov.html
http://www.phaos.com/
http://www.pki-page.org/
http://www.counterpane.com/pki-risks.html
http://www.shym.com
http://www.rsasecurity.com/rsalabs/pkcs/index.html
http://www.authentic8.com/
http://www.infosyssec.com/infosyssec/secpki1.htm
http://www.certco.com/
http://www.usertrust.com/
http://www.pkilaw.com/
http://www.dstc.qut.edu.au/MSU/projects/pki
http://www.dvnet.com/
http://www.infoseceng.com/corppki.htm
http://www.unicert.com/library/index.html
http://www.baltimore.co.uk/
http://www.entrust.com

Last updated: October 28, 2001

↑

Health Canada Santé Canada

Canada

Étude des technologies de protection des renseignements personnels

Préparé par Le Groupe EXOCOM inc.
Division de la stratégie d'entreprise et des services de consultation en TI
Pour le Bureau de la santé et l'inforoute
Santé Canada
30 août 2001

Table des matières

Résumé
1 Dossiers de Santé Électroniques : Caractéristiques et Utilisation
- 1.1 Infostructure de la santé et dossiers de santé électroniques
- 1.2 Questions de confidentialité
- 1.3 Élaboration de critères pour les technologies de protection des renseignements personnels

2 Etude des Technologies de Protection des Renseignments Personnels
- 2.1 Technologie de l'anonymat
- 2.2 Protocole de protection de la vie privée (P3P)
- 2.3 Infomédiaires et systèmes de gestion de l'identité
- 2.4 Systèmes de gestion de la confiance
- 2.5 Cartes intelligentes et cartes d'ordinateurs personnels
- 2.6 Biométrie et chiffrement biométrique
- 2.7 Infrastructure à clé publique et certificats numériques à clé publique

3 Applicabilité des Technologies d'Amélioration de la Confidentialité et Satisfaction aux Exigences de Protection des Reseignements Personnels
- 3.1 Responsabilité
- 3.2 Détermination des buts
- 3.3 Consentement
- 3.4 Limitation de la collecte
- 3.5 Limitation de l'utilisation, de la divulgation et de la conservation
- 3.6 Exactitude
- 3.7 Garanties
- 3.8 Ouverture
- 3.9 Accès personnel
- 3.10 Conformité

4 Conclusions et Recommandations
- 4.1 Généralités
- 4.2 TAC inappropriées
- 4.3 TAC appropriées
- 4.4 TAC prometteuses
- 4.5 Recommandations

Annexe A

Résumé

Le Groupe EXOCOM inc. a affecté deux directeurs au projet. Du mois de juin au mois d'août

2001, ils ont dirigé l'étude et l'évaluation. Divisées en quatre étapes, elles correspondent aux quatre sections du document.

Section 1 - Dossiers de santé électroniques : caractéristiques et utilisation

Les auteurs présentent un résumé des exigences du respect de la confidentialité dans le secteur de la santé en se basant sur des scénarios opérationnels et sur les dix principes d'information recommandés par le code de référence de protection de la confidentialité de l'Association canadienne de normalisation. Cette étape comprend des entrevues avec des membres du BSI et des discussions sur la conception générale d'un dossier de santé électronique, selon le BSI. Les résultats sont résumés, à la fin de la section 1, dans un tableau qui reprend les dix principes du respect de la confidentialité, les règles administratives liées à chacun de ces principes et les exigences auxquelles doivent satisfaire les technologies de protection des renseignements personnels pour soutenir ces règles administratives.

Section 2 - Étude des technologies

Les auteurs ont étudié les technologies de protection des renseignements personnels, déjà en vente ou disponibles bientôt sur le marché, pouvant appuyer les programmes de respect de la confidentialité. Les technologies retenues sont celles que les défenseurs du droit à la vie et les fournisseurs concernés qualifient généralement de technologies d'amélioration de la confidentialité, ainsi que celles qui, selon les auteurs, soutiennent certaines facettes de la protection des renseignements personnels. Les auteurs ont d'abord divisé les technologies retenues en six groupes ou familles technologiques. Ils ont ensuite décrit de quelle manière chacun de ces groupes protège les renseignements personnels et, finalement, ils ont évalué brièvement la pertinence d'utiliser ces technologies dans le contexte des dossiers de santé électroniques selon leur conception. À la suite de chaque description, les auteurs présentent une évaluation sommaire sous forme de tableau reprenant uniquement les dix principes de protection de la vie privée. Les auteurs indiquent avoir éprouvé des difficultés dans l'évaluation de certaines technologies de protection des renseignements personnels.

Section 3 - Évaluation des technologies

Cette section consiste essentiellement en un tableau détaillé des six groupes de technologies de protection des renseignements personnels, technologies comparées aux exigences décrites à la section 1 en utilisant l'évaluation faite de la pertinence à la section 2. Ce tableau est beaucoup plus détaillé que ceux de la section 2 puisque les auteurs y ont ajouté des commentaires sur le potentiel d'appui d'une technologie à une règle administrative lorsqu'elle est utilisée conjointement avec des applications ou d'autres infrastructures.

Section 4 - Conclusions et recommandations

Les auteurs formulent les conclusions de leur évaluation des technologies et recommandent l'examen des technologies les plus prometteuses en se basant sur les résultats de la section 3. Ils en concluent que les technologies les plus prometteuses sont les systèmes de gestion de la confiance et les infrastructures à clé publique, particulièrement lorsqu'elles sont utilisées conjointement et éventuellement avec des jetons. Les auteurs recommandent au BSI de mener quatre projets : examiner attentivement la possibilité d'utiliser un système de gestion de la confiance en association avec une infrastructure à clé publique; examiner la possibilité d'utiliser des jetons si de meilleures garanties et une attribution sont nécessaires ou si le concept final de dossier de santé électronique comporte l'exercice d'un contrôle de la part du patient sur une partie ou la totalité de son dossier médical; examiner la possibilité d'utiliser des infomédiaries si de multiples identités sont permises et élaborer un concept de dossier de santé électronique parallèlement aux autres projets.

L'annexe A est une liste partiellement annotée de sites Web utiles. Les annexes B à G inclusivement sont destinées à permettre aux personnes qui veulent en savoir davantage sur une technologie de s'informer en consultant des sites Web ou lisant les dépliants des

fournisseurs.

1 Dossiers de Santé Électroniques : Caractéristiques et Utilisation

1.1 Infostructure de la santé et dossiers de santé électroniques

Le secteur des soins de santé utilise la technologie afin d'améliorer les soins de santé prodigués aux Canadiennes et aux Canadiens où qu'ils soient, de même que pour accroître l'efficacité du régime de soins de santé. Les données qui correspondent aux besoins d'information du personnel du secteur de la santé, y compris les simples citoyens, feront partie de la vision de l'infostructure de la santé. Ces données proviendront de nombreuses banques de données du système de soins de santé, dont certaines vont produire des données auxquelles pourront accéder d'autres systèmes, y compris les systèmes utilisés pour le soutien administratif. Le Canada et d'autres pays occidentaux considèrent leurs systèmes de dossiers de santé électroniques (DSE) comme des éléments importants de l'infostructure de la santé. Les DSE offrent la possibilité d'atteindre de nombreux objectifs qui, au Canada, se résument ainsi :

- Ils permettent aux professionnels de la santé d'accéder rapidement, au besoin, au dossier d'un patient afin de lui donner de meilleurs soins;
- Les citoyens pourraient avoir accès à leur dossier de santé et seraient ainsi mieux en mesure de décider, conjointement avec les dispensateurs de soins de santé, de leurs soins de santé[1];
- Au moyen de garanties appropriées, les administrateurs de soins de santé, les décideurs et les chercheurs pourront utiliser les renseignements intégrés sur les soins de santé afin d'améliorer le système de soins de santé en réduisant les coûts, en tenant compte des développements futurs et en appuyant la recherche clinique et la recherche en service de santé.

Des groupes du secteur de la santé ont avancé le concept d'un DSE qui serait un dossier unique et longitudinal des visites qu'un patient a rendu à des dispensateurs de soins de santé. Selon le BSI, le DSE sera un dossier virtuel créé à partir de données sauvegardées à la source ou de données provenant de banques de données centralisées comme les recueils provinciaux de données proposés par les facultés de pharmacie. Le patient pourrait aussi avoir un dossier portatif contenant ses renseignements de santé personnels, tel que le groupe sanguin, les allergies et les contre-indications à certains médicaments, renseignements qui sont essentiels et nécessaires aux nombreux dispensateurs de soins de santé.

L'environnement des dossiers de santé utilise un large éventail de technologies et de possibilités technologiques, une variété de moyens, notamment les dossiers papier, et des normes et modèles divers pour des renseignements semblables. Ces systèmes de renseignements respectent et reflètent les différences de lois et de règlements auxquels ils sont assujettis. Dans le but de dresser une liste des exigences qui s'appliquent à la plupart des différents milieux, sinon à tous, les auteurs croient que l'infostructure idéale de la santé peut être et sera créée, et qu'elle sera même interopérable et totalement électronique, dans la mesure où les technologies d'amélioration de la confidentialité seront mieux appropriées dans ce contexte.

1.2 Questions de confidentialité

La législation et les codes relatifs à la protection de la vie privée sont conçus pour permettre aux citoyens d'éviter que leurs renseignements personnels soient utilisés sans leur consentement. Récemment, la législation relative à la protection de la vie privée a reconnu le droit de chaque citoyen de contrôler l'utilisation de ses renseignements personnels, c'est-à-dire la collecte, l'utilisation, la divulgation, la conservation et la disposition de ces renseignements par des agences de collecte de renseignements. Dans le contexte d'un DSE, les exigences en matière de protection de la vie privée, qui sont définies selon les dix principes[2] normalisés, représentent

un grand défi pour le secteur des soins de santé. Ces principes ne donnent pas de directives quant aux normes. Toutefois, ils en donnent quant aux règles administratives. Certaines exigences de ces dix principes sont difficilement applicables au secteur de la santé, principalement en ce qui concerne la propriété des renseignements par opposition aux dossiers qui renferment ses renseignements personnels et l'obligation d'aviser le patient des buts de la collecte des renseignements, d'obtenir son consentement et de l'aviser des modifications apportées à l'utilisation et au partage l'information avec une tierce partie.

1.3 Élaboration de critères pour les technologies de protection des renseignements personnels

Ce rapport reprend les règles administratives, comprises dans les dix principes de protection de la vie privée, pour établir les critères d'évaluation de l'utilité des technologies censées améliorer la confidentialité dans le contexte des soins de santé.
Le tableau ci-dessous donne la liste des exigences technologiques en appui aux règles administratives découlant des dix principes de protection de la vie privée. En fonction des exigences énumérées dans la troisième colonne, les auteurs déterminent si les technologies de protection de la vie privée favorisent effectivement cette protection dans le contexte des DSE.

Principes	*Règles administratives*	Exigences
1. Responsabilité *Un organisme est responsable des renseignements personnels se trouvant sous sa garde ou son contrôle et il devrait désigner une ou des personnes pour s'assurer du respect de ses principes.*	• Désigner une personne responsable • Exercer une responsabilité organisationnelle au sein de l'organisme • Exercer une responsabilité organisationnelle pour les renseignements personnels divulgués à des tierces parties	• Permettre à la personne responsable au sein de l'entreprise de gérer l'utilisation des renseignements personnels, leur divulgation, etc. • Vérifier le respect des principes, p. ex., liste de contrôle • Collecter et superviser l'état des contrôles utilisés dans la conduite d'autres principes • Faire rapport de l'état des contrôles, favoriser la gestion des questions de confidentialité
2. Détermination des buts *Les buts de la collecte de renseignements personnels doivent être déterminés au moment de la collecte ou avant.*	• Consigner les buts • Aviser les personnes du but de la collecte • Aviser les personnes de toute modification au but de la collecte • Dresser la liste des données et des buts	• Consigner les buts et faire le suivi de leurs modifications • Faciliter la tâche de la personne responsable • Consigner quand et comment les personnes sont avisées des buts et de leurs modifications
3. Consentement	• Prévoir des	• Consigner

La connaissance et le consentement de la personne sont requis pour la collecte, l'utilisation ou la divulgation de renseignements personnels.	méthodes visant à obtenir le consentement exprès de la personne s'il s'agit de renseignements personnels délicats • Conserver les détails des consentements - quand, comment, etc. • Conserver les détails des consentements retirés	l'historique des consentements accordés • Vérifier ou examiner la base de donnée des consentements
4. Limitation de la collecte *La collecte de renseignements personnels doit être limitée à ce qui est nécessaire aux buts précis. Les renseignements doivent être recueillis selon des moyens appropriés et légaux.*	• Décrire et consigner les méthodes de collecte retenues • Indiquer la source des renseignements • Chaque donnée doit être liée à un but et justifiée • La collecte des renseignements se fait en fonction d'un but précis	• Consigner de quelle manière chaque donnée correspond au but visé • Consigner la manière dont la collecte a été faite • Vérifier ou examiner la collecte • Enregistrer les raisons de la collecte des données • Enregistrer la méthode de collecte des données • Collecter les renseignements conformément aux règles et définitions fixées
5. Limitation de l'utilisation, de la divulgation et de la conservation *Les renseignements personnels ne doivent pas être utilisés ni divulgués à des fins autres que celles justifiant leur collecte, sauf avec le consentement de la personne ou tel que requis par la loi.*	**Utilisation :** • Exprimer tous les buts pour chaque dispensateur de soins de santé, par secteur • Déterminer qui, dans le secteur de santé, utilisera tel ou tel renseignement • Gérer l'accès aux données en fonction du rôle afin d'éviter que les données du but « a » servent au but « b» , etc.	**Utilisation :** • Consigner l'utilisation faite des renseignements • Consigner l'accès autorisé aux renseignements, définir les rôles • Gérer l'accès en fonction des autorisations • Vérifier l'accès et l'utilisation • Enregistrer qui peut avoir un accès • Permettre les accès autorisés et refuser tout autre

		accès • Enregistrer les demandes d'accès • Faire rapport des demandes d'accès qui n'ont pas reçu l'autorisation préalable
	Divulgation : • Établir un lien entre chaque accès ou divulgation et un but, puis le consigner • Gérer les exclusions – XXX ne doit pas avoir d'accès – et les consigner • Établir une liste des dossiers qui ne peuvent être divulgués ou utilisés par certains groupes • Assurer le traitement particulier des dossiers devant conserver l'anonymat (voir l'exemple du VIH)	**Divulgation :** • Refuser l'utilisation, l'accès ou la réception sur la base d'autorisations, de permissions et d'exclusions • Vérifier l'accès et la réception • Enregistrer les exclusions selon les règles d'autorisation ou de permission • Faire rapport des accès et réceptions par rôles exclus • Suivre les divulgations et réceptions autorisées
Les renseignements personnels doivent être conservés uniquement pour la période nécessaire à l'atteinte des buts et tel que requis par la loi.	**Conservation :** • Quelques dossiers de santé pourront être constitués et conservés plus longtemps afin de refléter l'espérance de vie (100 ans et plus) • Ententes de conservation selon le consentement obtenu • Élimination des dossiers et des copies de secours • Enregistrement des dossiers éliminés • Élimination ou destruction sûre	**Conservation :** • Consigner les règles de conservation • Consigner l'information relative à l'élimination des renseignements • Vérifier l'élimination de tous les renseignements recueillis lors d'une collecte • Vérifier la destruction des renseignements et l'attester • Consigner, tenir et gérer les enregistrements devant être conservés pendant longtemps • Inventorier toutes les copies (copies

		de secours, sous-ensembles, supports) • Consigner et enregistrer toutes les étapes du cycle de vie des collectes
6. Exactitude *Les renseignements personnels doivent être exacts et le plus à jour possible pour satisfaire les buts de leur collecte.*	• Procédures de validation des données • Maintien de l'intégrité • Mesures d'ouverture (Voir aussi le principe 9 ci-dessous : Accès personnel aux renseignements et capacité de les corriger)	• Vérifications de l'exactitude et de son maintien • Intégrité prévue dans les mécanismes de collecte et de conservation, pour toute collecte (Voir aussi le principe 9 ci-dessous)
7. Garanties *Les garanties de sécurité doivent protéger les renseignements personnels de la perte ou du vol, de même que des accès non autorisés, de la divulgation, de la copie, de l'utilisation ou de la modification à toutes les étapes de leur cycle de vie, quel que soit le support d'inscription.*	• Définir les exigences en matière de sécurité selon la nature délicate des renseignements et selon les conséquences de la perte, de la compromission ou de la corruption • Établir les besoins en fonction d'une procédure convenue d'EMR • Valider selon des normes de « meilleures pratiques » reconnues, p. ex : ISO17799 • Obtenir de l'information expliquant POURQUOI chaque garantie est nécessaire - ou non • Questions relatives aux garanties pour la tenue de dossiers pendant très longtemps (100 ans et plus) • Le matériel et les logiciels devront faire parties du « dossier », étant	• Diligence nécessaire en matière de protection des renseignements • Pratiques de sécurité reconnues (normes) • Objectifs supérieurs de confidentialité et d'intégrité • Droit d'accès très limité • Sélection des garanties en fonction des exigences • Les normes peuvent être HAZOP[3], ISO17799, Cobit ou toute autre norme reconnue • Outils spécifiques de protection des données justifiés pour atteindre les objectifs • Pour les dossiers de grande durée de vie, la récupération des données doit pouvoir se faire d'une génération de technologie à l'autre : si le matériel et les

	donné qu'ils sont nécessaires à la lecture de l'information	logiciels font partie du dossier, sa lecture en sera facilitée pour toute sa durée.
8. Ouverture *L'information précise au sujet des politiques et des pratiques relatives à la gestion des renseignements personnels doit être disponible à bref délai.*	• Le manuel des politiques est rendu public • Les changements de politique sont rendus publics pour satisfaire les besoins d'information • Nécessité de gérer les éléments publics par rapport aux éléments privés	• Mechanism(s) for policy accessibility
La personne concernée doit être informée de l'existence, de l'utilisation et de la divulgation de ses renseignements personnels.	• Informer de l'existence, de l'utilisation et de la divulgation • Nécessité d'une procédure visant à informer les personnes de l'état de la collecte (voir 2, 3 et 4) • Nécessité de conserver une liste des personnes ayant été informées et de celles qui ne peuvent l'être • Nécessité de conserver un relevé de l'utilisation fait afin d'informer les personnes concernées : à quel endroit les renseignements ont été utilisés, par qui et dans quel but • Nécessité de conserver un relevé des autres divulgations afin d'informer les personnes concernées • Nécessité de conserver un relevé des dates de destruction des	• Mécanismes permettant aux personnes de connaître l'état des renseignements, et d'y accéder, dont l'utilisation, la divulgation (y compris les personnes ayant accès à l'information) et la destruction. • Mécanismes permettant de conserver un relevé de la collecte, de l'utilisation, de la divulgation, des consentements et de la destruction.

	renseignements	
9. Accès personnel *Sur demande, une personne aura accès à ses renseignements personnels. Les exceptions au droit d'accès doivent être limitées et justifiées.*	• Consigner les exceptions • Méthodes permettant d'accorder à une personne l'accès à ses renseignements personnels • Méthodes permettant de vérifier l'identité des personnes	• Permettre aux personnes d'accéder à leurs renseignements; limiter les exceptions (identification et authentification) • Consigner qui fait la demande, quand et comment
La personne doit pouvoir remettre en question l'exactitude et l'exhaustivité de l'information à son sujet et la faire modifier si nécessaire.	• Consigner les raisons de toute modification à un dossier en mentionnant les renseignements avant et après la modification • Consigner les échéances s'il y a lieu • Consigner le moment où une personne a eu accès à ses renseignements et les résultats de cet accès • Nécessité d'autres preuves à l'appui	• Procédure de gestion des modifications sûre permettant d'enregistrer les demandes, d'y donner suite, de consigner les modifications et de les confirmer à la personne qui fait la demande • Mécanisme permettant de mettre à jour toutes les copies des collectes où figurent des renseignements sur la personne
10. Challenging Compliance *Une personne doit pouvoir remettre en question la conformité aux exigences relatives à la vie privée en s'adressant à une ou des personnes désignées.*	• Étayer la procédure de remise en question de la conformité, y compris les mécanismes de réponse et les responsabilités • Méthode permettant de traiter les remises en question et de les gérer • Étayer la procédure d'amendement des pratiques relatives à la protection de la vie privée	• Vérifier les remises en question de la conformité et les réponses

2 Etude des Technologies de Protection des Renseignments Personnels

Les technologies de protection de renseignements personnels doivent fournir aux organismes des moyens de gérer les procédures entourant cette protection, à la fois pour leur personnel et pour les personnes qui fournissent ces renseignements. Notre démarche dans cette évaluation a consisté à déterminer les dispositifs ou les fonctions que doivent posséder les outils automatisés afin d'appuyer les principes et les objectifs de protection de la vie privée. La section 1 du rapport présente ces exigences.

Les systèmes de DSE sont conçus pour recueillir des renseignements sur la santé. Par défaut, la plupart de ces renseignements concernent la personne et ils doivent être gérés et traités conformément aux principes reconnus de protection de la vie privée. Les exigences de cette protection diffèrent des exigences nécessaires à la gestion de l'information médicale des DSE.

Les technologies de protection des renseignements personnels, ou technologies d'amélioration de la confidentialité(TAC)[4], l'expression employée pour la recherche sur le Web, visaient d'abord la protection de l'identité des personnes lors de la consultation de sites Web, d'interactions ou des transactions sur le Web. Même si ces outils de préservation de l'anonymat peuvent jouer un rôle dans la façon d'accéder à l'information médicale, ils peuvent s'avérer inappropriés dans un contexte où des données personnelles doivent être associées à des personnes précises et lorsque l'accès doit être restreint à des personnes autorisées. Cela s'applique aux DSE où la création, la modification, le partage, la communication et la destruction des données sur la santé d'une personne s'adressent et se limitent à des personnes autorisées.

De nouvelles méthodes pointent à l'horizon. Certaines, comme les cartes intelligentes, constituent de nouvelles façons d'utiliser la technologie de la sécurité actuelle afin d'améliorer la confidentialité. Cette section décrit ce qui est généralement considéré une technologie propre à la protection des renseignements personnels ainsi que sa capacité à appuyer les règles de protection de la vie privée. Il importe également de noter que la technologie peut servir à appuyer les politiques, les processus et les procédures, mais qu'elle ne les remplace pas.

Cette section fait état de six grandes catégories de technologies de protection des renseignements personnels. Chaque catégorie décrite ci-dessous est accompagnée d'une évaluation sommaire de la manière dont la technologie en question peut ou non favoriser la confidentialité. L'annexe A est une bibliographie partiellement annotée de sites Web traitant des technologies de protection des renseignements personnels. Les annexes B à H inclusivement présentent de l'information précise provenant des fournisseurs et des exemples des produits disponibles pour chacune des six catégories. Les tableaux respectifs de l'évaluation des technologies de cette section indiquent si, à grande échelle, la conception d'une technologie donnée peut ou non appuyer les règles administratives de protection des renseignements personnels. Pour certaines technologies, la conception d'un DES et le rôle joué par le patient dans le contrôle de ses renseignements personnels influenceront leurs capacités à satisfaire une exigence de protection de la vie privée. La section 3 présente une analyse plus détaillée du potentiel d'une technologie donnée pour appuyer les règles administratives de protection des renseignements personnels.

2.1 Technologie de l'anonymat

L'anonymat se définit comme étant le refus de dévoiler son identité. Les services d'anonymat (anonymizer) remplacent l'identité des utilisateurs d'Internet par un identificateur temporaire qui demeure en fonction lors de l'accès seulement. Ainsi, tout renseignement personnel fourni par l'utilisateur ne peut pas servir à le retracer.

Le fonctionnement des services d'anonymat part du principe que les menaces de violation de la vie privée sur Internet proviennent d'une surveillance non autorisée des activités en ligne, de l'ignorance de la journalisation de ces activités, de la conservation de ces journaux d'activités pour un usage ultérieur et de la divulgation de l'information recueillie à des parties inconnues. La surveillance et la journalisation de nombreux sites Internet peuvent produire d'énormes quantités d'informations pouvant être accumulées et traitées à différentes fins qui demeurent inconnues de l'intéressé. Les utilisateurs perdent ainsi le pouvoir de choisir ce qu'ils veulent divulguer à leur

sujet, le pouvoir de décider à qui ces renseignements et activités sont destinés et à quel usage ils serviront. L'anonymat offre à l'utilisateur d'Internet la possibilité de visiter des sites Web et de faire des transactions sans révéler sa véritable identité ou ses intérêts. Ainsi, l'information recueillie sur ses habitudes de navigation sur le Web perd tout son sens.

Dans Internet, l'anonymat peut prendre l'une ou l'autre des formes suivantes : un anonymat permanent, ou pseudonyme, lorsque l'utilisateur revêt une identité permanente qui n'est pas liée à son nom, ou un anonymat ponctuel lorsque l'utilisateur revêt une autre identité le temps d'une activité en ligne. Dans les deux cas, l'information ne peut être associée au nom réel de l'utilisateur, quoique, dans le cas du pseudonyme, de nombreuses activités en ligne peuvent être liées à ce pseudonyme. Les techniques d'anonymat simples comptent le recours à un tiers de confiance, qui efface l'en-tête des messages Internet et retransmet leur contenu en utilisant son identificateur, ainsi que la connexion à un serveur de messagerie et la falsification des en-têtes qui sont attachées au message. Les retransmetteurs anonymes combinent ces deux techniques en utilisant un ordinateur qui automatise le processus de remplacement des en-têtes et de retransmission. Dans la plupart des cas, l'ordinateur de l'usager cache un lien qui relie son pseudonyme à son nom véritable, d'où la nécessité de contrôles de sécurité pour protéger ce lien. Les retransmetteurs anonymes protègent ce pseudonyme plus ou moins efficacement.

Des techniques et des intermédiaires de confiance peuvent minimiser la nécessité de collecter des renseignements personnels ou minimiser le nombre de fois où l'accès aux renseignements est requis. La nouvelle technologie de retransmission anonyme améliore la protection contre l'interception illicite grâce à des techniques comme le chaînage et le chiffrement de chaque lien de la chaîne et les messages de longueur identique. Certaines techniques peuvent empêcher les requêtes répétées et les attaques de corrélation passive et utiliser continuellement le trafic aléatoire généré pour dissimuler les vrais messages. Les serveurs utilisant les pseudonymes assurent un anonymat supplémentaire en ayant recours aux réserves d'identités des retransmetteurs anonymes et au chiffrement. Les réserves de messages protègent les utilisateurs en leur permettant de chiffrer un message à l'aide de la clé publique du destinataire avant de l'envoyer à une liste d'envoi ou à un groupe de discussion. Les retransmetteurs anonymes peuvent aussi être utilisés pour la navigation anonyme sur Internet : un serveur mandataire peut filtrer les en-têtes d'identification et repérer l'origine des envois à partir d'un navigateur Web.

En ce qui concerne le commerce électronique, la technologie de protection de l'identité et des renseignements personnels est prometteuse. La caisse électronique anonyme, comme la DigiCash, utilise la cryptographie pour protéger l'identité du payeur et assurer ainsi la protection de ses renseignements personnels. Selon toute vraisemblance, le concept d'anonymat utilisé par différents services se traduira par des infrastructures acceptant l'anonymat bidirectionnel, tel que le réseau de retransmission anonyme, et désignées parfois sous le nom de protocole Pipenet. À ce jour, la nature du protocole Pipenet ne protège pas suffisamment des attaques habituelles dirigées contre les retransmetteurs anonymes et associées à des connexions dont le temps d'attente est court et la durée, longue. Cependant, certains systèmes de cartes de crédit sur Internet permettent à l'utilisateur de payer un achat par carte de crédit sans transmettre son numéro de carte de crédit directement au vendeur.

Évaluation des technologies de l'anonymat

Pour les DSE virtuels, les technologies de l'anonymat ont un potentiel limité, principalement à cause de leur vulnérabilité actuelle aux attaques. Les techniques de transaction anonyme par carte de crédit peuvent s'avérer utiles dans le traitement des autorisations de paiement des services de santé, à la condition que cela fasse partie d'un DSE. Les hypothèses implicites relatives aux technologies de l'anonymat sont de fait contraires à certaines exigences d'un DSE. Les services d'anonymat cachent l'identité alors que l'identité est une exigence des DSE. Le tableau ci-dessous résume en quoi les technologies de l'anonymat répondent aux exigences de confidentialité d'un DSE.

Principes	Applicabilité

Responsabilité	Non - pas selon les paramètres de conception; les services d'anonymat ne peuvent pas accepter la vérification; ni superviser les contrôles puisqu'il est impossible d'instaurer des contrôles s'il n'y a pas d'attribution.
Détermination des buts	Non - pas selon les paramètres de conception
Consentement	Non - pas selon les paramètres de conception
Limitation de la collecte	Non - pas selon les paramètres de conception
Limitation de l'utilisation, de la divulgation et de la conservation	Non - la conception est contraire à l'attribution de l'action; les services d'anonymat ne peuvent accepter la vérification; ni superviser les contrôles puisqu'il est impossible d'instaurer des contrôles s'il n'y a pas d'attribution.
Exactitude	Non - pas selon les paramètres de conception
Garanties	Non - pas selon les paramètres de conception
Ouverture	Non - pas selon les paramètres de conception
Accès personnel	Non - pas selon les paramètres de conception
Remise en question de la conformité	Non - pas selon les paramètres de conception

2.2 Protocole de protection de la vie privée (P3P)

Le protocole de protection de la vie privée a été élaboré par le Consortium de normalisation du Web W3C afin d'établir une procédure automatisée permettant aux utilisateurs d'exercer un contrôle sur l'utilisation de leurs renseignements personnels qui sont recueillis lorsqu'ils consultent des sites Web. Parmi les créateurs du P3P se trouvent une multitudes de fournisseurs et autres, dont America Online/Netscape, American Express, le commissaire à l'information et à la protection de la vie privée de l'Ontario, Microsoft, Citibanque, IBM, NEC, Nokia, et le commissaire à la protection de la vie privée de Schleswig-Holstein. Le consortium W3C croit que le P3P sera bientôt en mesure de constituer la norme attendue.

Le P3P est un outil conçu pour permettre aux fournisseurs de commerce électronique de concevoir des services qui respectent le droit à la vie privée de l'utilisateur et ses préférences. Il permet aussi aux utilisateurs en ligne de mieux contrôler la confidentialité de leurs données grâce aux choix individualisés concernant les relations qu'ils veulent établir avec les services offerts sur le Web. Le P3P fonctionne selon un ensemble de politiques et de règles ne protégeant pas nécessairement en soi la confidentialité. Dans les pays qui, comme le Canada, sont dotés de lois protégeant le droit à la vie privée, le P3P peut servir à évaluer les énoncés de confidentialité. En effet, il permet de collecter et d'analyser ces énoncées, puis d'évaluer leur conformité. Le P3P permet également d'améliorer la transparence et l'exactitude, mais il ne peut garantir que les organisations respectent les politiques de protection des renseignements personnels.

Le P3P définit un ensemble de pratiques normalisées pour la collecte de renseignements personnels. Les sites Web déterminent de quelles façons ils entendent traiter les données recueillies. Les utilisateurs déterminent, à l'aide de questions à choix multiples, de quelles façons ils souhaitent que leurs renseignements personnels soient recueillis et traités. Les navigateurs dotés du P3P peuvent alors comparer les choix d'un utilisateur avec les politiques du site Web. Ils permettent à l'utilisateur de consulter le site tout en connaissant les différences entre ses préférences et celles du site. Un langage d'échange des préférences du P3P (APPEL) est utilisé pour encoder les préférences de l'utilisateur et les politiques du site, et pour prendre directement des mesures appropriées.

Les utilisateurs peuvent aussi se servir des fonctionnalités du P3P pour emmagasiner les

données qu'ils échangent fréquemment avec des sites Web.

De nouveaux concepts laissent présager que le P3P servira de base à la conception de systèmes de gestion de l'identité qui permettront à l'utilisateur de gérer son droit à la vie privée et de contrôler son identité électronique. Ce concept est repris au paragraphe 2.4 ci-dessous.

Évaluation du P3P

Le P3P a été créé pour aider les utilisateurs à évaluer de quelle façon un site Web traite leurs renseignements personnels. Il peut également aider les organismes à élaborer des politiques et des pratiques de protection de la confidentialité. La technologie du P3P peut aider le secteur de la santé à élaborer et à gérer des politiques de protection des renseignements personnels lorsque ces renseignements sont échangés dans Internet, par des portails ou des sites Web, y compris la façon dont l'information est partagée entre les services liés. Ce protocole pourrait assurer la cohérence.

La plus grande faiblesse du P3P tient au fait qu'il ne peut garantir que les organismes vont respecter leurs propres politiques. La technologie ne possède pas de dispositifs de sécurité telles que le contrôle de l'accès, l'identification et l'authentification. En outre, il est conçu pour l'échange direct entre l'utilisateur et le site Web. Le P3P offre un soutien limité au modèle courant de DSE, et uniquement si le BSI a prévu que le patient jouera un rôle direct dans l'autorisation de l'établissement de liens entre ses données et dans la gestion de leurs enregistrements. L'évaluation de la capacité du P3P à accepter les principes de protection de la vie privée représente tout un défi. Le P3P couvre l'aspect de l'examen des politiques seulement, mais n'offre pas de dispositifs de sécurité. Son utilité dépend également du rôle accordé au patient lors de la conception du DSE. Le tableau ci-dessous n'évalue par conséquent que les aspects de la mise en application connus de l'utilisateur.

Principes	**Applicabilité**
Responsabilité	Non - ne fait pas partie des paramètres de conception
Détermination des buts	Oui - en autant que les politiques sont respectées
Consentement	Éventuellement - en fonction de la conception du DSE : les patients ont le choix de fournir l'information demandée s'ils sont d'accord avec les politiques; toutefois rien ne garantit le respect des politiques.
Limitation de la collecte	Éventuellement - en fonction de la conception du DSE : seulement l'information que le patient accepte de donner est recueillie, en autant que les politiques sont respectées et qu'aucune procédure imprévue n'a été mise au point pour recueillir des renseignements supplémentaires.
Limitation de l'utilisation, de la divulgation et de la conservation	Non - ne fait pas partie des paramètres de conception
Exactitude	Non - ne fait pas partie des paramètres de conception
Garanties	Non - ne fait pas partie des paramètres de conception
Ouverture	Oui - si les politiques sont respectées; les politiques sont vérifiées au moyen des outils du P3P
Accès personnel	Non - ne fait pas partie des paramètres de conception
Remise en question de la conformité	Non - ne fait pas partie des paramètres de conception

2.3 Infomédiaires et systèmes de gestion de l'identité

Quelques entreprises sont à l'origine d'outils et de services conçus pour aider l'utilisateur à gérer son identité en ligne. Ces intermédiaires de l'information - les infomédiaires - offrent des outils qui permettent aux utilisateurs de conserver des renseignements personnels dans un emplacement sûr. Cette information peut alors être utilisée, grâce au remplissage automatique de formulaire, pour limiter l'information que les utilisateurs veulent partager avec les sites ayant une politique de protection des renseignements personnels qui correspond à leurs préférences. Certains fournisseurs « engendrent» des infomédiaires en établissant des entreprises qui agissent précisément comme infomédiaires. Les uns semblent s'orienter principalement vers la gestion de la relation avec le client, bien que leurs produits mettent de l'avant le maintien et le respect du consentement du client lorsque l'information est échangée. Les autres ont intégré la biométrie à leur solution et offrent des portefeuilles électroniques ou d'autres formes de caisses électroniques.

Certains outils infomédiaires sont basés sur le P3P. Les protocoles P3P, lorsqu'ils sont associés à un réseau de communication anonyme, offre des systèmes de gestion de l'identité. Ces outils permettent à l'utilisateur qui préfère utiliser des noms différents selon les contextes de gérer ses multiples combinaisons d'identités, de fonctions et de données personnelles. Les systèmes de gestion de l'identité permettent à l'utilisateur de décider quelles données transmettre à telle personne, quand agir de façon anonyme, quand utiliser un pseudonyme et quand révéler son identité ou authentifier des données. Certains systèmes proposent des pseudonymes certifiés pouvant être utilisés lorsqu'une véritable identité est requise. C'est le cas, par exemple, d'une transaction commerciale, d'un vote à une élection, d'un achat préautorisé, de l'enregistrement d'une garantie, etc. Les certificats peuvent être transférés ou utilisés comme pièces justificatives, vérifiés en ligne et assortis d'une date d'expiration au besoin.

Dans le cas d'infomédiaires bien structurés, seul l'utilisateur ou le propriétaire de l'information peut établir un lien avec son pseudonyme. Toutefois, les données sont emmagasinées à un seul emplacement et pourraient être extraites et analysées par les infomédiaires qui voudraient obtenir un portrait détaillé des habitudes de l'utilisateur. Les systèmes permettant cette fonction de recoupement des données présentent donc un potentiel d'ingérence dans la vie privée.

Évaluation des infomédiaires et des systèmes de gestion de l'identité

En combinant la gestion de l'identité aux services d'anonymat et aux techniques du P3P, cette technologie permet aux utilisateurs d'Internet de gérer leurs différentes identités. Cette même technologie doit toutefois respecter les principes de protection des renseignements personnels afin de permettre aux utilisateurs de décider de la façon dont leurs renseignements personnels sont diffusés. Ces outils ne correspondent pas tout à fait aux exigences de gestion de la confidentialité décrites au tableau 1, soit parce que les systèmes qu'ils utilisent permettent un accès par pseudonyme, soit parce qu'ils contiennent des renseignements personnels.

Sur le plan de la technologie de l'anonymat, l'objectif des infomédiaires et des systèmes de gestion de l'identité est de dissocier l'utilisateur de ses renseignements personnels. Cet aspect de la technologie semble donc ne pas pouvoir satisfaire le but principal des systèmes de DSE virtuels, soit assurer la disponibilité instantanée de toute l'information concernant une personne aux parties autorisées.

Les auteurs croient que les infomédiaires pourraient jouer un rôle dans les systèmes de DES, même s'ils ne sont pas conçus à cette fin. De telles bases de données sur l'identité pourraient servir à établir des liens entre les enregistrements d'une personne. Il suffirait de suivre les différents identificateurs utilisés par cette personne dans les différentes bases de données qui ont alimenté le DSE. Cela permettrait au responsable ou propriétaire de chaque base de données sur la santé de gérer l'information de la manière la plus efficace possible et de fournir cette information à d'autres professionnels de la santé sans restriction exagérée. Si l'infomédiaire avait la capacité d'enregistrer l'usage fait de l'information, les patients auraient ainsi un certain contrôle sur l'information recueillie à leur sujet, à condition que la conception du DSE permette aux patients de jouer un rôle direct dans leur DSE.

Principes	Applicability
Responsabilité	Non - ne fait pas partie des paramètres de conception
Détermination des buts	Éventuellement - à condition que les politiques des P3P et autres soient établies et respectées
Consentement	Éventuellement - en fonction de la conception du DSE : les patients ont le choix de fournir l'information demandée en utilisant leur identité réelle ou un pseudonyme
Limitation de la collecte	Éventuellement - à condition que les politiques des P3P et autres soient établies et respectées
Limitation de l'utilisation, de la divulgation et de la conservation	Éventuellement - en fonction de la conception du DSE, et si la création d'une base de données sur l'identité et de multiples identités est permise; outil permettant d'enregistrer l'usage fait de l'information
Exactitude	Non - pas selon les paramètres de conception
Garanties	Non - pas selon les paramètres de conception
Ouverture	Oui - à condition que les politiques des P3P et autres soient respectées
Accès personnel	Éventuellement - en fonction de la conception du DSE et si l'usage fait de l'information est enregistré
Remise en question de la conformité	Non - pas selon les paramètres de conception

2.4 Systèmes de gestion de la confiance

Un système de gestion de la confiance permet aux applications de répondre à des interrogations telles que « Cette opération potentiellement dangereuse est-elle conforme à mes politiques de sécurité?» . Généralement, la bonne réponse dépend du type d'opérations, de celui qui la demande, des politiques de sécurité locales, des justificatifs d'identité du demandeur et d'autres facteurs encore. Les systèmes de gestion de la confiance dotent les applications d'une interface normalisée en mesure de donner des réponses à de telles interrogations. Ces systèmes permettent aussi aux utilisateurs de rédiger, dans un langage normalisé, les politiques et les justificatifs d'identité qui contrôlent ce qui est permis de faire et ce qui ne l'est pas. Un système de gestion de la confiance est composé de cinq éléments :

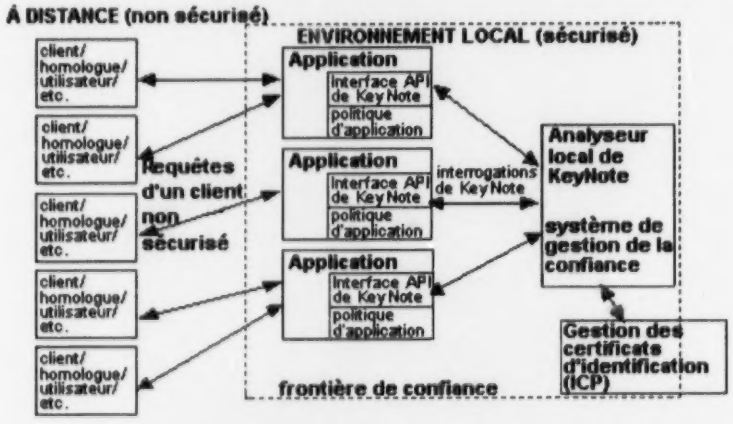
- Un langage permettant de décrire les activités, soit les opérations qui ont des répercussions sur la sécurité et qui sont prises en charge par le système;
- Un mécanisme d'identification des mandants, soit les entités qui sont autorisées à effectuer des opérations[5];
- Un langage permettant de préciser les politiques d'application, qui régissent les activités que les mandants sont autorisés à effectuer;
- Un langage permettant de déterminer les justificatifs d'identité, qui permettent aux mandants de déléguer l'autorisation à d'autres mandants;
- Un vérificateur de conformité, qui dotent les applications d'un mécanisme qui détermine la manière de traiter une activité demandée par un mandant, compte tenu des politiques et d'un ensemble de justificatifs d'identité.

Dans les applications conventionnelles, les politiques sont souvent incorporées au programme et difficiles à changer. Dans un système de gestion de la confiance, les politiques sont rédigées dans un langage normalisé. Ce langage demeure le même pour toutes les applications, il est défini parallèlement au code de l'application et peut être changé, au besoin, par l'utilisateur responsable. L'unification des notions de politiques de sécurité et de justificatifs d'identité forme un concept particulièrement puissant. Les applications disponibles peuvent facilement générer

des politiques qui renvoient à une autorité de télégestion pouvant changer la politique en délivrant simplement de nouveaux justificatifs d'identité (certificats). Une politique peut devenir, par sa seule signature, un certificat utilisable à distance.

Le recours à un système de gestion de la confiance, pour superviser les services de sécurité stratégiques, évite au concepteur d'applications de devoir considérer toute une série de questions subtiles, et souvent difficiles, en matière de conception et d'implémentation. Cela permet aussi aux utilisateurs de tirer profit d'un langage d'application indépendant, flexible et normalisé pour préciser les politiques. Avant la venue de la gestion de la confiance, les applications devaient avoir leurs propres mécanismes de spécification des politiques, d'analyse des justificatifs d'identité et d'association de l'authentification de l'utilisateur avec l'autorisation d'effectuer des opérations « risquées» . Les systèmes de gestion de la confiance sont dotés d'une interface qui se charge éventuellement de tous ces aspects. Le concepteur d'applications n'a plus qu'à cerner les questions de gestion de la confiance dans l'application et à formuler les interrogations appropriées au système de gestion de la sécurité.

Le schéma ci-dessous, extrait de la vue d'ensemble de l'architecture de gestion de la confiance de KeyNote, illustre le mode de fonctionnement de cette technologie :



Architecture de gestion de la confiance de KeyNote

Évaluation des systèmes de gestion de la confiance

La gestion de la confiance réunit les notions de politique de sécurité, de justificatif d'identité, de contrôle de l'accès et d'autorisation. Une application qui utilise un système de gestion de la confiance peut simplement demander au vérificateur de la conformité si la demande d'activité peut être autorisée. Il pourrait s'agir, par exemple, de l'accès requis par les mandants pour la gestion des renseignements personnels.

En outre, les politiques et les justificatifs d'identité sont écrits dans des langages normalisés, partagés par toutes les applications de gestion de la confiance; le mécanisme de configuration de la sécurité d'une application donnée possède la même structure sémantique et syntaxique qu'une autre application, même lorsque la sémantique des applications diffère quelque peu. Les politiques de gestion de la confiance peuvent être diffusées facilement dans les réseaux, évitant ainsi de devoir diffuser des mécanismes de configuration des politiques propres aux applications, des listes de contrôle des accès et des programmes d'analyse et d'interprétation des justificatifs d'identité[6].

Cette technologie semble offrir plusieurs des dispositifs essentiels aux systèmes de DSE pour faciliter la gestion de l'accès aux renseignements personnels et à leur utilisation. La gestion de la confiance ajoute cependant une certaine complexité à la gestion des renseignements personnels sans toutefois fournir les contrôles requis pour recueillir les renseignements selon les

dix principes de protection de la confidentialité.

Principles	Applicabilité
Responsabilité	Oui - Les règles de confiance peuvent être conçues de façon à assurer le consentement, à limiter l'utilisation et la divulgation, à protéger d'autres accès et à permettre l'accès à l'intéressé. Ces règles peuvent faire l'objet d'une vérification, assurant ainsi la responsabilité requise pour la protection de la confidentialité. Le recours à l'infrastructure à clé publique (ICP) pour l'authentification peut fournir des garanties sur l'identité des utilisateurs et des administrateurs.
Détermination des buts	Oui - des certificats peuvent être créés pour chaque but visé
Consentement	Oui - peut être intégré à la procédure de création des certificats
Limitation de la collecte	Oui - par la conception (voir détermination des buts) et par la vérification
Limitation de l'utilisation, de la divulgation et de la conservation	Oui - association de justificatifs d'identité, de la gestion de l'accès assistée par l'ICP, de la journalisation et de la vérification
Exactitude	Oui - en utilisant les certificats numériques de l'ICP pour l'intégrité; les personnes préposées à la collecte ne peuvent pas modifier les renseignements sauf si elles détiennent les certificats appropriés.
Garanties	Partiellement - fournit des mécanismes de contrôle de l'accès
Ouverture	Non - seulement dans l'énoncé des politiques; ne fait pas partie des paramètres de conception
Accès personnel	Oui - les personnes qui fournissent les renseignements pourraient avoir un certificat leur permettant d'accéder à leur information selon la conception des DES; les utilisateurs ayant le certificat approprié peuvent vérifier l'exactitude des données.
Remise en question de la conformité	Non - ne fait pas partie des paramètres de conception

L'annexe E donne des exemples de systèmes de gestion de la confiance.

2.5 Cartes intelligentes et cartes d'ordinateurs personnels

La technologie des cartes intelligentes a progressé au point où la capacité de mémoire accrue et la fonctionnalité permettent la création de solutions sécurisées pour tout un éventail de situations. Les cartes intelligentes sont utilisées depuis le début des années 70 pour de nombreux types d'application. Sous leur forme la plus courante, elles conservent en mémoire des données pouvant être transmisses lorsqu'elles sont placées dans un lecteur ou, dans leur version la plus récente, lorsqu'elles se trouvent à proximité d'appareils qui captent les radiofréquences. De nombreuses versions de cartes intelligentes comprennent des protocoles de cryptographie complexes qui les rendent aptes à protéger la confidentialité de l'information mémorisée.

Les cartes intelligentes peuvent être utilisées pour emmagasiner l'information d'un justificatif

d'identité, tel que les titres universitaires, les cotes de solvabilité et les autorisations d'accès à une pièce, et pour prouver que la personne détient ce justificatif d'identité sans avoir à révéler les renseignements personnels normalement requis pour la vérification des justificatifs d'identité. En Europe, les cartes intelligentes sont largement utilisées pour effectuer des transactions par le biais d'applications de vente, de téléphonie et de récupération d'information et, principalement, à titre de « porte-monnaie» électroniques. Les cartes de Personal Computer (PC), Personal Computer Memory Card International Association (PCMCIA), Miniature, SmartMedia, MultiMedia et CompactFlash offrent différentes capacités de mémoire et varient aussi bien en taille qu'en compatibilité avec les services de connecteurs et de cartes.

Les cartes intelligentes peuvent emmagasiner l'information qui définit l'identité d'une personne. En se servant d'un lecteur, une personne peut certifier son identité à un système informatisé afin de récupérer ou d'emmagasiner de l'information. Une telle interface liée à un système de contrôle d'accès ou à une infrastructure de gestion des autorisations peut être utilisée pour permettre un accès autorisé à l'information en fonction des règles établies au préalable. Ces cartes peuvent aussi conserver en mémoire des enregistrements de renseignements personnels. Toute personne souhaitant accéder à cette information doit avoir la carte en sa possession ainsi que l'autorisation de lire l'information qu'elle contient. Bien que les auteurs n'aient pas indiqué quels appareils peuvent effectuer ces opérations, les cartes intelligentes ayant une programmation appropriée peuvent enregistrer les données relatives à l'utilisation et à l'accès. Ce dispositif d'enregistrement des activités permettrait aux cartes intelligentes de satisfaire aux nombreuses exigences relatives à la protection de la confidentialité et à l'établissement de rapport qui ont été décrites précédemment.

Évaluation des cartes intelligentes et des cartes d'ordinateurs personnels

Même si la technologie des cartes intelligentes permet de conserver des dossiers médicaux et qu'elle aide les utilisateurs à gérer l'accès à ces dossiers, les utilisations les plus courantes de la technologie se limitent à la mise en mémoire de l'information utilisée pour certifier l'identité de son propriétaire ou des clés de chiffrement permettant de chiffrer l'information. Beaucoup reste à faire toutefois avant que la technologie des cartes intelligentes n'assure la gestion des renseignements personnels.

Principles	**Applicabilité**
Responsabilité	Non - ne fait pas partie des paramètres de conception
Détermination des buts	Non - ne fait pas partie des paramètres de conception
Consentement	Non - ne fait pas partie des paramètres de conception
Limitation de la collecte	Non - ne fait pas partie des paramètres de conception
Limitation de l'utilisation, de la divulgation et de la conservation	Non - ne fait pas partie des paramètres de conception
Exactitude	Partiellement - si la carte possède une signature numérique
Garanties	Partiellement -vérification de l'identité très sûre
Ouverture	Non - ne fait pas partie des paramètres de conception
Accès personnel	Non - ne fait pas partie des paramètres de conception à moins que la conception du DSE prévoie un accès à jeton pour le patient
Remise en question de la conformité	Non - ne fait pas partie des paramètres de conception

L'annexe F donne des exemples de cartes intelligentes.

2.6 Biométrie et chiffrement biométrique

L'avènement de la biométrie [7] qui a recours aux empreintes digitales, à l'empreinte vocale et à la lecture d'empreinte rétinienne, laisse présager un très haut niveau de sécurité lors des procédures de d'identification des personnes. Un appareil biométrique authentifie la personne et vérifie son accessibilité à un service ou à une information précise. La vérification biométrique remplace le mot de passe ou le NIP et offre l'avantage d'une authentification plus sûre que le mot de passe ou le NIP pour contrer l'usurpation d'identité. Le contrôle des représentations biométriques numériques mises en mémoire, de même que de leurs clés de cryptage lorsque la cryptographie est utilisée, constitue le point faible de ce système. L'information provenant de diverses sources peut encore être liée ou associée au modèle de référence biométrique, permettant ainsi à des tiers d'avoir accès à des profils personnels complets et détaillés.

Le chiffrement basé sur une clé biométrique peut être utilisé pour rendre l'information anonyme dans une banque de données en isolant l'identité de la personne de ses renseignements personnels. Le lien entre l'identité et l'information est un pointeur qui est encodé par le dactylogramme de la personne, par exemple, ou par une autre représentation biométrique. La personne contrôle maintenant ces renseignements personnels.

Certaines techniques biométriques n'offrent pas la stabilité voulue pour une utilisation généralisée à grande échelle. Les empreintes digitales ou rétiniennes peuvent changer selon les conditions ou les blessures dues à des accidents, perdant ainsi leur caractère sûr. La lecture d'empreinte rétinienne s'avère la solution la plus prometteuse, même si la plupart des Canadiennes et des Canadiens y sont réticents, la considérant comme une intrusion. La technologie de la reconnaissance vocale fait également de grands progrès et a été intégrée à plusieurs applications de moindre envergure. La technologie biométrique est toutefois relativement coûteuse.

Évaluation de la biométrie et du chiffrement biométrique

La biométrie et le chiffrement biométrique offrent des possibilités d'identification et d'authentification très sûres lorsqu'ils sont utilisés conjointement avec une carte à puce ou des cartes d'ordinateurs personnels, et éventuellement avec une infrastructure à clé publique ou des systèmes de gestion de la confiance. La biométrie assure la meilleure identification et la meilleure authentification des personnes autorisées à accéder à un DSE pour le consulter ou en extraire des données. Dans le cas des organismes de soins de santé, comme les hôpitaux, ce niveau de granularité peut ne pas être garanti, à moins que le patient utilise une carte pour permettre la saisie ou l'extraction de données. Bien des personnes considèrent la biométrie comme une intrusion et elles sont réticentes à y recourir alors que d'autres considèrent qu'elle ne contrevient pas au droit à la vie privée.

L'utilisation de la biométrie dans un système de DSE exige que des ingénieurs d'application se préoccupent de la manière dont l'enregistrement biométrique est emmagasiné aux fins de copie de secours. De plus, l'enregistrement adéquat des personnes représente un grand défi, particulièrement si les appareils biométriques doivent être utilisés en grand nombre.

Principes	Applicabilité
Responsabilité	Non - ne fait pas partie des paramètres de conception
Détermination des buts	Non - ne fait pas partie des paramètres de conception
Consentement	Non - ne fait pas partie des paramètres de conception

Limitation de la collecte	Non - ne fait pas partie des paramètres de conception
Limitation de l'utilisation, de la divulgation et de la conservation	Non - ne fait pas partie des paramètres de conception
Exactitude	Partiellement - si la carte possède une signature numérique
Garanties	Partiellement -authentification de l'identité très sûre
Ouverture	Non - ne fait pas partie des paramètres de conception
Accès personnel	Non - ne fait pas partie des paramètres de conception, sauf si le patient peut exercer un contrôle sur son dossier de santé électronique
Remise en question de la conformité	Non - ne fait pas partie des paramètres de conception

L'annexe G donne des exemples de systèmes biométriques.

2.7 Infrastructure à clé publique et certificats numériques à clé publique

Les certificats numériques à clé publique (certificats) font partie de l'infrastructure à clé publique (ICP). Ils requièrent normalement que l'identité d'une personne soit validée suivant différents degrés de rigueur et qu'elle soit liée à la signature numérique et aux certificats de confidentialité délivrés par une autorité de certification (AC). La clé publique d'une personne est conservée dans un répertoire qui est accessible à toute personne détenant un certificat reconnu par le répertoire. Les ICP offrent un éventail de services de sécurité, incluant le chiffrement, la signature numérique, la non-répudiation, l'identification et l'authentification. Les nouvelles versions d'ICP offrent de nombreux dispositifs, dont la gestion des autorisations.

Les infrastructures à clé publique rendent possible l'utilisation des applications permettant de chiffrer les données et de signer numériquement les messages. Les infrastructures à clé publique sont fondées sur les principes de la cryptographie à clé publique. La cryptographie à clé publique permet de chiffrer de l'information grâce à deux clés reliées mathématiquement : l'une d'elles demeure privée et l'autre est rendue publique. La clé privée ne peut être déduite de la clé publique. Par exemple, une personne qui veut envoyer un message utilise la clé publique du destinataire afin de chiffrer le message. Le destinataire utilise sa clé privée pour déchiffrer le message. L'expéditeur a donc l'assurance que seul le destinataire voulu peut lire le message.

La cryptographie à clé publique peut aussi servir à créer des signatures numériques. La signature numérique d'un message s'obtient à l'aide d'une fonction mathématique qui calcule une valeur en fonction du contenu du message. Cette valeur est ensuite annexée au message et chiffrée au moyen de la clé privée de l'expéditeur. Le destinataire du message déchiffre alors la signature numérique au moyen de la clé publique de l'expéditeur et obtient la valeur annexée au message en utilisant la fonction mathématique de l'expéditeur. Si la signature numérique peut être déchiffrée et si les deux valeurs annexées sont identiques, le destinataire est assuré à la fois de l'identité de l'expéditeur et de l'intégrité du message. Comme la signature numérique d'un message est étroitement associée à la clé privée de son expéditeur, il lui est donc plus difficile de répudier ce message.

Les clés sont gérées par une autorité de certification, qui peut être tiers de confiance chargé d'associer une biclé publique/privée à une entité ou un particulier donné, appelée un abonné. Cette autorité délivre et révoque des certificats et conserve des listes des certificats révoqués. Les certificats numériques, portant la signature numérique de l'autorité de certification, renferment la clé publique et prouvent que la personne identifiée au certificat détient la clé privée

correspondante. Deux autorités de certification ou plus peuvent être liées par une certification croisée afin de pouvoir reconnaître réciproquement les certificats délivrés par différents organismes.

De nombreux dispositifs d'une ICP constituent une intrusion dans la vie privée, notamment l'enregistrement des clés publiques dans un répertoire accessible à tous ceux qui détiennent une clé délivrée par une autorité de certification ou par des autorités de certification liées par une certification croisée. Cette technologie peut éventuellement être conçue pour accepter la protection de la confidentialité en utilisant des pseudonymes ou toute autre méthode visant à dissimuler l'identité du détenteur du certificat. Les procédures d'enregistrement lient toutefois la véritable identité du détenteur du certificat au certificat.

Évaluation de l'infrastructure à clé publique

L'ICP est une technologie relativement bien maîtrisée qui, lorsqu'elle est utilisée conjointement avec d'autres technologies, s'annonce très prometteuse pour les DSE. Même si les ICP requièrent des efforts considérables pour leur mise en application, notamment une attention marquée apportée à la gestion, aux politiques et aux pratiques, elles offrent plusieurs caractéristiques qui permettront aux DSE de respecter les principes de protection de la vie privée, soit l'identification et l'authentification, la non-répudiation, la gestion des politiques, les normes et la confidentialité. Une infrastructure de gestion des autorisations peut être utilisée conjointement à l'ICP.

Une mise en œuvre réussie de l'ICP requiert une gestion solide des politiques au sein d'un organisme, de l'autorité de certification et entre les organisations liées par une certification croisée. Des exigences de vérification et des normes font partie intégrante de l'ICP. Cette dernière exige également que les abonnés acceptent de protéger leur clé en signant une entente formelle. Celle-ci pourrait constituer en même temps un consentement officiel pour la collecte et l'utilisation de quelques renseignements personnels. L'ICP offre aussi la possibilité de déployer une infrastructure permettant à des appareils, plutôt qu'à des personnes, d'accéder aux données, d'en ajouter ou d'en changer.

L'association étroite entre le certificat délivré par une ICP et l'identité de son destinataire, l'abonné, est habituellement considérée contraire aux principes de protection de la confidentialité. Si les patients sont abonnés, alors les répertoires représentent une source de violation potentielle de la confidentialité, à moins d'utiliser un identificateur ou une autre méthode. Le Secrétariat du Conseil du Trésor examine actuellement des façons de régler ce problème. Pour rendre ce modèle mesurable, il est nécessaire d'adopter un mode uniforme d'enregistrement des abonnés et de délivrance des certificats.

Malgré qu'elles soient bien maîtrisées, les ICP sont des outils servant à vérifier l'identité des personnes avant de les autoriser à accéder à des renseignements précis ou à des ressources de traitement de l'information. En soi, cette technologie ne satisfait pas aux exigences ni aux principes de protection de la vie privée déjà mentionnés. Cependant, l'ICP permet d'identifier les abonnés avec une grande certitude. Les interfaces d'application reliant ces identités aux enregistrements des DSE servent à éviter que des données personnelles ne tombent entre les mains de personnes non autorisées.

Il est difficile de mesurer la capacité de l'ICP à satisfaire aux exigences de protection de la confidentialité, car l'ICP dépend grandement des politiques, de la gestion des politiques et des garanties. Les politiques et la vérification, ainsi que la gestion des politiques, servent d'automatismes régulateurs; les politiques doivent être conçues pour respecter le caractère confidentiel et les vérifications doivent être publiques. Le fardeau des politiques qui accompagnent l'ICP se complique davantage si une infrastructure de gestion des autorisations est utilisée, même si la gestion des autorisations peut aider l'ICP à répondre aux exigences de protection des renseignements personnels. L'évaluation ci-dessous indique à quel niveau les politiques peuvent être vérifiées pour se conformer aux exigences de protection de la vie privée; sur quel plan la conception du DSE et le rôle du patient dans son DSE peuvent déterminer si l'ICP répond aux exigences et sur quel plan une infrastructure de gestion des autorisations

permettra à l'ICP de satisfaire aux exigences de protection des renseignements personnels.

Principes	Applicabilité
Responsabilité	Oui - vérification et gestion des politiques
Détermination des buts	Oui - les politiques de certificat et l'énoncé des pratiques de certification peuvent fixer les buts et définir les normes de respect des buts fixés; vérification
Consentement	Éventuellement - si les certificats délivrés aux patients et si l'entente signée par l'abonné incluent l'acceptation des conditions des politiques du certificat
Limitation de la collecte	Éventuellement - si l'infrastructure de gestion des autorisations est utilisée
Limitation de l'utilisation, de la divulgation et de la conservation	Éventuellement - si l'infrastructure de gestion des autorisations est utilisée et que les politiques de certificat énoncent que l'utilisation, la divulgation, la conservation et la vérification peuvent être retracées. Une solution doit être trouvée au problème des répertoires (voir le texte ci-dessus)
Exactitude	Partiellement - par le biais de la conservation des enregistremetns portant une signature numérique
Garanties	Oui - permet la vérification de l'identité, le chiffrement pour préserver la confidentialité et les signatures numériques pour assurer la responsabilité (non-répudiation)
Ouverture	Oui - les politiques de certificat, qui doivent être soumises à la vérification, et les résultats de la vérification doivent être rendus publics
Accès personnel	Éventuellement - si les patients sont autorisés à accéder à une infrastructure de gestion des autorisations
Remise en question de la conformité	Non - ne fait pas partie des paramètres de conception

L'annexe A donne des exemples d'ICP.

3 Applicabilité des Technologies d'Amélioration de la Confidentialité et Satisfaction aux Exigences de Protection des Reseignements Personnels

Résumé des résultats

Cette section résume les exigences de protection des renseignements personnels présentées à la section 1, suivant les dix principes de protection de la confidentialité, et indique les technologies pouvant éventuellement satisfaire à chacune des exigences. Le tableau ci-dessous propose des méthodes, autres que la conception, qui répondent ou pourraient répondre aux exigences. Lorsque la conception de la TAC satisfait à une exigence, les auteurs l'indique en caractères gras.

Exigences	TAC applicables[8]

3.1 Responsabilité	
1. Permettre à la personne responsable au sein de l'entreprise de gérer l'utilisation des renseignements personnels, leur divulgation, etc.	P3P - Si les politiques sont respectées et la vérification possible, peut y avoir une gestion des politiques entre les autorités et les systèmes **ICP - vérification et gestion des politiques** **Systèmes de gestion de la confiance - Conception de l'ICP accepte l'identification et l'authentification; règles pouvant être vérifiées**
2. Vérifier le respect des principes, p. ex., liste de contrôle	**ICP - signatures numériques (non-répudiation) comprises dans l'infrastructure de gestion des autorisations;** **vérification des systèmes de gestion de la confiance - conception : vérification**
3. Collecter et superviser l'état des contrôles utilisés dans la conduite d'autres principes	**ICP - exigences de vérification des politiques de certificat et vérification de l'infrastructure de gestion des autorisations** **SYSTÈMES DE GESTION DE LA CONFIANCE - CONCEPTION : VÉRIFICATION**
4. Faire rapport de l'état des contrôles, favoriser la gestion des questions de confidentialité	**ICP -vérification et gestion des politiques** **SYSTÈMES DE GESTION DE LA CONFIANCE - CONCEPTION : VÉRIFICATION**
3.2 Détermination des buts	
1. Consigner les buts et faire le suivi de leurs modifications	P3P si les politiques sont respectées Infomédiaires - si des politiques du type P3P sont respectées **ICP - gestion des politiques de certificat et des politiques; vérification** **SYSTÈMES DE GESTION DE LA CONFIANCE - CONCEPTION : CRÉER DES CERTIFICATS DIFFÉRENTS POUR CHAQUE BUT DÉTERMINÉ**
2. FACILITER LA TÂCHE DE LA PERSONNE RESPONSABLE	**ICP - CRÉATION D'UNE AUTORITÉ DE GESTION DES POLITIQUES ET PUBLICATION DES POLITIQUES DE CERTIFICAT; VÉRIFICATION** **Gestion de la confiance - conception : vérification de l'utilisation des certificats**
3. CONSIGNER QUAND ET COMMENT LES PROPRIÉTAIRES DE L'INFORMATION SONT AVISÉES DES BUTS ET DE LEURS MODIFICATIONS	P3P ET INFOMÉDIAIRES - SI LES POLITIQUES SONT RESPECTÉES **ICP - POLITIQUES DE CERTIFICAT; ÉVENTUELLEMENT PAR ENTENTE AVEC L'ABONNÉ SI LE PATIENT EST ABONNÉ; VÉRIFICATION**
3.3 Consentement	
1. Consigner l'historique des consentements accordés	P3P - dépend de la conception du DSE et du respect des politiques;

	Infomédiaires - dépend de la conception du DES ICP - éventuellement par entente avec l'abonné si le patient est abonné **Gestion de la confiance - fait partie de la création du certificat** Biométrie/chiffrement biométrique - utilisation personnelle de la biométrie pouvant être un consentement tacite; l'utilisation devrait être consignée Carte intelligente - comme pour la biométrie
2. Vérifier ou examiner la base de données des consentements	ICP - maintien des ententes avec l'abonné lorsque les patients sont abonnés (manuel) **Gestion de la confiance - Vérification de la base de données des justificatifs d'identité**
3.4 Limitation de la collecte	
1. Consigner de quelle manière chaque donnée vient corroborer le but visé	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement – politiques de certificat, ententes avec l'abonné lorsque le patient est abonné, infrastructure de gestion des autorisations **Gestion de la confiance - voir « Détermination des buts» (3.2)**
2. Consigner la manière dont la collecte a été faite	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement – politiques de certificat, modèle d'enregistrement, ententes avec l'abonné lorsque le patient est abonné, vérification **Gestion de la confiance - voir « Détermination des buts»**
3. Vérifier ou examiner la collecte	**ICP - exigences de vérification des politiques de certificat** **Gestion de la confiance - voir « Détermination des buts»**
4. Enregistrer les raisons de la collecte des données	ICP - éventuellement par des politiques de certificat et ententes avec l'abonné lorsque le patient est abonné **Gestion de la confiance - voir « Détermination des buts»**
5. Enregistrer la méthode de collecte des données	ICP - politiques de certificat et ententes avec l'abonné lorsque le patient est abonné **Gestion de la confiance - voir « Détermination des buts»**
6. Collecter les renseignements conformément aux règles et définitions fixées	P3P et infomédiaires - si des politiques sont mises en place ICP - politiques de certificat, modèle d'enregistrement, ententes avec l'abonné lorsque le patient est abonné **Gestion de la confiance - voir « Détermination des buts»** Biométrie - si le patient exerce un

	contrôle sur son DSE
3.5 Limitation de l'utilisation, de la divulgation et de la conservation	
Utilisation	
1. Consigner l'utilisation faite des renseignements	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement par la gestion des autorisations, politiques de certificat **Gestion de la confiance - par les justificatifs d'identité**
2. Consigner l'accès autorisé aux renseignements, définir les rôles	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement par la gestion des autorisations **Gestion de la confiance - par les justificatifs d'identité**
3. Gérer l'accès en fonction des autorisations	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement par une infrastructure de la gestion des autorisations **Gestion de la confiance - par les justificatifs d'identité**
4. Vérifier l'accès et l'utilisation	ICP : éventuellement par la gestion des autorisations, exigence de vérification des politiques de certificat, journal des intrusions **GESTION DE LA CONFIANCE : PAR LES JUSTIFICATIFS D'IDENTITÉ, EXAMEN DU VÉRIFICATEUR DE LA CONFORMITÉ**
5. Enregistrer qui peut avoir un accès	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement par une infrastructure de la gestion des autorisations **Gestion de la confiance - par les justificatifs d'identité**
6. Permettre les accès autorisés et refuser tout autre accès	**ICP - Identification et authentification**; éventuellement par une infrastructure de la gestion des autorisations **Gestion de la confiance - par les justificatifs d'identité + ICP pour les contrôles d'accès et la vérification**
7. Enregistrer les demandes d'accès	**ICP - journaux des accès à la base de données ou des intrusions** **GESTION DE LA CONFIANCE - JOURNAUX DES ACCÈS À LA BASE DE DONNÉES DE L'ICP OU JOURNAUX DES INTRUSIONS**
8. Faire rapport des demandes d'accès n'ayant pas reçu l'autorisation préalable	**ICP - politiques de certificat, énoncé des pratiques de certification, garanties, journaux et alertes d'intrusion** **Gestion de la confiance - journaux des**

	accès à la base de données de l'ICP
Divulgation	
1. Refuser l'utilisation, l'accès ou la réception sur la base d'autorisations, de permissions et d'exclusions	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement par l'intégration de l'identification et de l'authentification conjointement à une infrastructure de gestion des autorisations **Gestion de la confiance - par les justificatifs d'identité et les contrôles d'identification et d'autorisation de l'ICP** Chiffrement biométrique - justificatifs d'identité pour les entités autorisées ou contrôle des patients par carte intelligente biométrique si le patient exerce un contrôle sur son DSE
2. Vérifier l'accès et la réception	**ICP - contrôles d'identification et d'autorisation** **GESTION DE LA CONFIANCE - CONTRÔLES D'IDENTIFICATION ET D'AUTORISATION DE L'ICP**
3. Consigner les exclusions selon les règles d'autorisation ou de permission	P3P et infomédiaires - si des politiques sont mises en place **ICP - par la gestion des autorisations et les contrôles d'identification et d'autorisation** **Gestion de la confiance - par les justificatifs d'identité et les contrôles d'identification et d'autorisation de l'ICP**
4. Faire rapport des accès et réceptions par rôles exclus	**ICP - par la gestion des autorisation et les contrôles d'identification et d'autorisation; journal des accès à la base de données** **GESTION DE LA CONFIANCE - PAR LES JUSTIFICATIFS D'IDENTITÉ ET LES CONTRÔLES D'IDENTIFICATION ET D'AUTORISATION DE L'ICP; JOURNAL DES ACCÈS À LA BASE DE DONNÉES**
5. Suivre les divulgations et réceptions autorisées	**ICP et gestion des autorisations - journal des accès à la base de données**
Conservation	
1. Consigner les règles de conservation	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement par des politiques de certificat, énoncé des pratiques de certification Gestion de la confiance - politiques
2. Consigner la manière dont seront éliminés les renseignements	P3P et infomédiaires - si des politiques sont mises en place ICP - éventuellement par des politiques de certificat, énoncé des pratiques de certification Gestion de la confiance - politiques

3. Vérifier l'élimination de tous les renseignements recueillis lors d'une collecte	ICP - exigences de vérification des politiques de certificat Gestion de la confiance - exigences de vérification
4. Vérifier la destruction des renseignements et l'attester	ICP - politiques de certificat, énoncé des pratiques de certification Gestion de la confiance - par l'ICP comme ci-dessus
5. Consigner, tenir et gérer les enregistrements devant être conservés pendant longtemps	ICP - politiques de certificat, énoncé des pratiques de certification, services de notaire Gestion de la confiance - par l'ICP comme ci-dessus
6. Inventorier toutes les copies (copies de secours, sous-ensembles, supports)	ICP - politiques de certificat, énoncé des pratiques de certification Gestion de la confiance - par l'ICP comme ci-dessus
7. Consigner et enregistrer toutes les étapes du cycle de vie des collectes	ICP - politiques de certificat, énoncé des pratiques de certification Gestion de la confiance - par l'ICP comme ci-dessus
3.6 Exactitude	
Vérifications de l'exactitude et de son maintien	Cartes intelligentes et biométrie : si la signature numérique est utilisée, journaux des utilisations ICP - partiellement par des enregistrements portant une signature numérique **GESTION DE LA CONFIANCE - LES PERSONNES PRÉPOSÉES À LA COLLECTE NE PEUVENT PAS MODIFIER L'INFORMATION, SAUF SI ELLES DÉTIENNENT LES JUSTIFICATIFS D'IDENTITÉ + UNE SIGNATURE NUMÉRIQUE APPROPRIÉS POUR PRÉSERVER L'INTÉGRITÉ**
Intégrité prévue dans les mécanismes de collecte et de conservation, pour toute collecte	Cartes intelligentes et biométrie : si la signature numérique est utilisée ICP - partiellement par la signature numérique **Gestion de la confiance - les personnes préposées à la collecte ne peuvent pas modifier l'information, sauf si elles détiennent les justificatifs d'identité + une signature numérique appropriés pour préserver l'intégrité**
Voir « Accès personnel» (3.9) et capacité de corriger l'information	
3.7 Garanties	
1. Diligence nécessaire en matière de protection des renseignements	Cartes intelligentes et biométrie - si les cartes peuvent chiffrer, une signature numérique; recours à l'identification et à l'authentification **ICP - chiffrement, signature numérique - degré de certitude**

	approprié Gestion de la confiance - par l'ICP
2. Pratiques de sécurité reconnues (normes)	Cartes intelligentes et biométrie - si les cartes peuvent chiffrer, signature numérique; recours à l'identification et à l'authentification **ICP - Énoncé des pratiques de certification pour le chiffrement, la signature numérique, la sécurité physique, les ententes avec l'abonné; ententes de certification croisée; sécurité personnelle, physique et technique** **Gestion de la confiance - fournit des mécanismes de contrôle de l'accès**
3. Objectifs supérieurs de confidentialité et d'intégrité	Cartes intelligentes et biométrie - si les cartes peuvent chiffrer, signature numérique; recours à l'identification et à l'authentification **ICP - CONCEPTION : CHIFFREMENT, SIGNATURE NUMÉRIQUE, NON-RÉPUDIATION, COPIE DE SECOURS** Gestion de la confiance - utilisation de l'ICP pour les garanties
4. Droit d'accès très limité	Cartes intelligentes et biométrie - utilisation de l'identification et de l'authentification **ICP - identification et authentification, modèle d'enregistrement**; éventuellement par une gestion des autorisations **Gestion de la confiance - justificatifs d'identité Biométrie, chiffrement biométrique pour un contrôle de l'accès plus serré** au besoin
5. Sélection des garanties en fonction des exigences	Cartes intelligentes et biométrie - si les cartes peuvent chiffrer, signature numérique; recours à l'identification et à l'authentification - s'ajoutent à d'autres garanties **ICP - garanties, en fonction de la sélection d'un degré de certitude approprié** Gestion de la confiance - par l'ICP
6. Les normes peuvent être HAZOP, ISO17799, Cobit ou toute autre norme reconnue	Comme ci-dessus
7. Outils spécifiques de protection des données justifiés pour atteindre les objectifs	**ICP - sélection d'un degré de certitude approprié** Gestion de la confiance - par l'ICP
8. Pour les dossiers de longue durée, la récupération des données doit pouvoir se faire d'une génération de technologie à l'autre : si le matériel et les logiciels font partie du dossier, sa lecture en sera facilitée pour	CP - services de notaire peuvent favoriser le maintien de l'intégrité du document Gestion de la confiance - éventuellement par services de notaire

toute sa durée	
3.8 Ouverture	
1. Mécanismes d'accessibilité aux politiques	**P3P et infomédiaires - publication des politiques; accessibles pour permettre l'appariement des politiques entre les organismes partageant les renseignements** **ICP - publication des politiques de certificat et des vérifications**
2. Mécanismes permettant aux personnes de connaître l'état des renseignements, et d'y accéder, dont l'utilisation, la divulgation (y compris les personnes ayant accès à l'information) et la destruction	P3P et infomédiaires - examen des politiques seulement Gestion de la confiance et ICP - Voir « Accès personnel» (3.9)
3. Mécanismes permettant de conserver un relevé de la collecte, de l'utilisation, de la divulgation, des consentements et de la destruction	**ICP - VÉRIFICATION DE LA GESTION DES AUTORISATIONS, JOURNAUX DES INTRUSIONS ET DES DEMANDES D'ACCÈS À LA BASE DE DONNÉES**
3.9 Accès personnel	
1. Permettre aux propriétaires de l'information d'accéder à leurs renseignements; limiter les exceptions (identification et authentification)	Infomédiaires - en fonction de la conception du DSE et si l'information relative à l'utilisation est consignée **Jetons : biométrie, chiffrement biométrique - carte intelligente ou carte d'ordinateur personnel du patient lui permettant d'accéder à son DSE lorsqu'il exerce un contrôle sur celui-ci (voir « Gestion de la confiance» ci-dessous)** ICP - partiellement par l'identification et l'authentification lorsque le patient est abonné; jeton éventuellement requis **GESTION DE LA CONFIANCE - LA PERSONNE QUI FOURNIT DES RENSEIGNEMENTS DEVRAIT DÉTENIR UN JUSTIFICATIF D'IDENTITÉ POUR POUVOIR Y ACCÉDER SELON LA CONCEPTION DU DSE**
2. Consigner qui fait la demande, quand et comment	**ICP - journal des intrusions; journal des demandes d'accès à la banque de données** **Gestion de la confiance - comme pour l'ICP**
3. Procédure de gestion des modifications sûre permettant d'enregistrer les demandes, d'y donner suite, de consigner les modifications et de les confirmer aux propriétaires de l'information	ICP - permet des modifications aux politiques par l'autorité de gestion des politiques et l'affichage public des politiques de certificat Gestion de la confiance - comme pour l'ICP
4. Mécanisme permettant de mettre à jour toutes les copies des collectes où figurent des renseignements sur la personne	ICP - changements à la gestion des autorisations, possibilité de délivrer à nouveaux des certificats **Gestion de la confiance - conception**

3.10 Conformité	
1. Vérifier les remises en question de la conformité et les réponses	

4 Conclusions et Recommandations

4.1 Généralités

La conception des technologies actuelles de protection des renseignements personnels ne répond pas aux exigences fonctionnelles qui découlent de la législation et des codes en matière de protection de la vie privée. Aucune des technologies étudiées ne peut fournir les outils appropriés permettant aux gestionnaires de la protection des renseignements personnels de répondre aux questions fondamentales concernant l'information confidentielle qu'ils détiennent : quelle utilisation en fait-on? qui y a accès? quand a eu lieu le dernier accès? la collecte est-elle sûre et acceptable? et ainsi de suite. Comme il faillait s'y attendre, aucune TAC ne répond à toutes les exigences et aucun outil ne répond exactement aux remises en question de la conformité. Cela est dû en partie au fait que les défis administratifs trouvent leur source à l'extérieur du DSE. Tel qu'il a été mentionné dans l'introduction, les auteurs reconnaissent que la technologie seule comble uniquement quelques exigences. Pour certaines toutefois, comme les technologies de l'anonymat et le protocole de protection des renseignements personnels, aucune technologie intégrée ne vient appuyer les politiques. Les cartes intelligentes et la biométrie utilisées seules ne peuvent satisfaire que quelques exigences, mais elles permettent de maximiser les TAC prometteuses.

Plusieurs des outils décrits ont une fonctionnalité qui se limite à dissimuler l'identité des utilisateurs ou à permettre la création et la gestion de nombreux pseudonymes servant à dissimuler l'identité réelle de la personne. Les auteurs croient que cela ne correspond pas aux exigences des DSE voulant que les enregistrements soient clairement associés à une personne, à des fins d'intégrité et de responsabilité. Par conséquent, ils en concluent que les services d'anonymat, les protocoles de protection des renseignements personnels et les infomédiaires ne conviennent pas aux DSE.

D'autres technologies, comme l'ICP, répondent aux exigences de protection des renseignements personnels principalement grâce à l'application de politiques et d'ententes avec l'abonné. Cette technologie exige qu'une attention soit portée aux politiques, procédures et processus. De plus, elle devra intégrer une gestion des politiques et de la gouvernance ainsi que la vérification de la conformité à tout le moins. L'interopérabilité sera également une question de technologie et de budget. La technologie basée sur l'adhésion volontaire aux politiques de protection des renseignements personnels a besoin également de s'étoffer davantage pour s'assurer du respect des politiques. Les outils étudiés n'avancent pas de politiques ni ne donnent l'assurance qu'ils ne seront pas contournés. Pour les systèmes de gestion de la confiance, les politiques sont transmises à toutes les applications et la technologie qui renforcera la gestion des autorisations et les autres exigences de politiques est disponible actuellement. Les personnes chargées de concevoir les DSE et les systèmes de DSE doivent donc se renseigner sur les politiques.

Malgré le fait que de nombreux outils contribuent à protéger les renseignements personnels, les auteurs concluent que cette contribution se limite habituellement à un objectif très restreint qui, dans bien des cas, crée un conflit de gouvernance au sein des DSE. Aucun outil ne fournit aux administrateurs de la protection des renseignements personnels le soutien dont ils ont besoin pour vérifier que l'application utilisée par un organisme respecte ces principes.

En partant des principes de protection de la vie privée, les auteurs ont établi un certain nombre d'exigences qui devront être ajoutées aux spécifications commerciales conventionnelles des applications. Le tableau de la section 3 présente un bon nombre de ces exigences. Seules les

applications qui tiennent compte de la protection des renseignements personnels, au moment de leur conception, peuvent satisfaire tous les besoins de cette protection. Les six catégories de technologies de protection des renseignements personnels de la section 2 sont reprises ci-dessous selon l'évaluation faite par les auteurs de leur capacité à accepter les exigences de protection de la confidentialité.

4.2 TAC inappropriées

Certaines TAC ne conviennent pas aux DSE. Nous recommandons de ne pas utiliser ces outils dans le contexte actuel de la santé.

Services d'anonymat (anonymizers)

Les services d'anonymat, par leur conception, ne permettent pas l'attribution d'activités comme la saisie ou l'extraction de données. Les DSE se conformant aux politiques exigerait qu'à tout le moins quelques actions soient attribuées à une personne ou à un organisme, mais il est impossible d'assurer la responsabilité. En outre, les services d'anonymat n'offrent aucune autre protection pour garantir la disponibilité, la confidentialité et l'intégrité des enregistrements, des transactions et des autres aspects des DSE. Bien que des garanties puissent être ajoutées, l'incapacité d'assurer la responsabilité est suffisamment sérieuse pour évaluer que cette technologie n'a aucun potentiel d'utilisation dans les DSE, ni maintenant ni plus tard.

Protocole de protection des données personnelles (P3P)

Bien que le P3P facilite la tâche des organismes dans l'élaboration de pratiques et de politiques conformes à la protection de la confidentialité, il n'offre aucune assurance aux utilisateurs de DSE et aux patients relativement à la conformité. Comme c'est le cas pour les services d'anonymat, le P3P ne protège pas l'information au moyen de contrôles de l'accès, du chiffrement et d'autres garanties de sécurité normalisées. Ces dispositifs pourraient être ajoutés, mais l'application des politiques demeure incertaine. Cette incertitude constitue une sérieuse limitation à l'ouverture véritable et à la responsabilité et elle limite l'utilisation, la divulgation et la conservation. Cela signifie que le P3P offre peu, sinon rien, aux DSE.

Infomédiaires et systèmes de gestion de l'identité

La gestion de l'identité associée aux infomédiaires ne permet pas à un système de DSE fondé sur cette technologie de choisir implicitement la responsabilité. En outre, les systèmes basés sur le P3P, la majorité, ne seront pas en mesure d'assurer la conformité. Les infomédiaires et les systèmes de gestion de l'identité ont une possibilité d'utilisation limitée dans les DSE, selon leur conception, et pourraient servir à gérer de multiples identités lorsque celles-ci sont permises.

4.3 TAC appropriées

Certaines TAC possèdent des dispositifs utiles qui pourraient être incorporés à une autre technologie dans le cadre des DSE.

Cartes intelligentes et cartes d'ordinateur personnel

Ces technologies sont capables de renforcer le contrôle de l'accès par une identification et une authentification sûres et elles pourraient servir à faciliter la gestion des autorisation. Cette technologie, dont l'utilisation est analogue aux cartes de crédit et de débit, devrait être examinée pour le potentiel qu'elle représente, étant donné sa grande acceptation par des utilisateurs moins bien informés.

Biométrie

Cette technologie, lorsqu'elle est associée aux cartes intelligentes, pourrait améliorer les contrôles de l'accès et la gestion des autorisations. La mise en mémoire de l'information biométrique devra être faite avec le plus grand soin. L'enregistrement à grande échelle des personnes pose un sérieux défi. Cette technologie pourrait s'avérer efficace si les DSE doivent permettre au patient un certain accès à ses renseignements personnels. À l'heure actuelle, certaines formes de biométrie sont moins acceptables que d'autres.

4.4 TAC prometteuses

Deux types de technologie méritent qu'on s'y attarde plus en détail : les systèmes de gestion de la confiance et les infrastructures à clé publique.

Systèmes de gestion de la confiance

Les systèmes de gestion de la confiance offrent un certain nombre de dispositifs intéressants, notamment la gestion des autorisations et l'application de la politique de conformité. Cette technologie permet également la création d'un système de DSE conçu pour répondre aux exigences particulières du secteur de la santé grâce à l'utilisation d'un langage indépendant de l'application et à des interfaces simples. L'association des politiques et des justificatifs d'identité permet la responsabilité, le contrôle de l'accès et la gestion des autorisations. L'un des aspects les plus intéressants de la gestion de la confiance est que la sécurité des TI et la conformité aux politiques de protection de la confidentialité sont indépendantes de l'application, contrairement à l'ICP (voir ci-dessous). Cette technologie devrait être examinée plus avant afin de bien déterminer son potentiel d'utilisation pour les DSE et de déterminer ses faiblesses éventuelles.

Infrastructures à clé publique (ICP)

Les infrastructures à clé publique sont essentiellement un outil permettant de valider l'identité des personnes qui souhaitent accéder à des ressources spécifiques : dossiers, courriers électroniques, autorisations, etc. Une identité valide permet alors à l'application de vérifier la responsabilité des actions prises au cours d'une collecte et d'un traitement de renseignements personnels. Cette technologie offre l'avantage d'être plutôt bien comprise et elle est en cours d'application dans de nombreuses sphères d'activité, y compris au gouvernement fédéral et dans plusieurs provinces. La conservation des renseignements personnels dans un répertoire de l'ICP constitue en soi une question de protection de la confidentialité, étant donné que le répertoire s'enrichit continuellement de nouvelles données au sujet des certificats et de leur détenteur.

Une attention particulière doit être accordée à la gestion des politiques et à la gouvernance des ICP qui dépendent des abonnés pour préserver la confidentialité de leurs clés privées. Certains nouveaux outils sont plus sévères pour l'enregistrement et la délivrance de certificats. Le nombre d'applications qui acceptent l'ICP augmente, mais les applications devront probablement être codées pour accepter le chiffrement, les signatures numériques, la gestion des autorisations et d'autres outils. Cette technologie mérite d'être examinée plus attentivement afin de déterminer son potentiel d'utilisation pour les DSE ainsi que la possibilité de neutraliser ou de réformer certains de ses dispositifs de protection de la confidentialité non conviviaux.

Solution combinée

L'association technologique la plus prometteuse pour les DSE semble être celle de la gestion de la confiance et de l'ICP, améliorée avec l'utilisation éventuelle des cartes intelligentes et de la biométrie. L'ICP peut offrir plusieurs des garanties requises, telles qu'un chiffrement sûr pour la confidentialité et les signatures numériques. La conception d'une gestion de la confiance peut permettre la diffusion des certificats, utilisés par les composantes du contrôle de l'accès, afin de renforcer les pratiques appuyant la protection de la confidentialité. Certains outils internes de gestion ayant été intégrés à ces types de système peuvent réellement fournir de l'information sur les pratiques de protection de la confidentialité faisant partie intégrante de l'application.

4.5 Recommandations

Des recommandations détaillées ne peuvent pas vraiment être avancées à ce point de l'évaluation des technologies de protection des renseignements personnels. En général, les recommandations suivantes consistent à retenir les technologies qui laissent présager qu'elles répondront aux exigences de protection de la confidentialité en appui aux politiques adéquates et à écarter les technologies qui donnent moins d'assurance à ce sujet.

Première recommandation : Le BSI devrait examiner de manière approfondie les systèmes de gestion de la confiance et l'infrastructure à clé publique.
Deuxième recommandation : Le BSI devrait considérer l'utilisation des cartes intelligentes et, éventuellement, de la biométrie pour améliorer la protection des renseignements personnels lorsque des limitations strictes de l'accès et d'autres actions sont requises.
Troisième recommandation : Lorsque de multiples identités sont permises, le BSI devrait considérer la possibilité d'utiliser des infomédiaires.
Quatrième recommandation : Les activités mentionnées ci-dessus devraient se faire parallèlement à l'élaboration du concept de DSE de manière à ce que la technologie et les exigences soient créées ensemble.

---

[1] La plupart des organismes envisagent de restreindre l'accès au patient, lorsque l'avis d'un dispensateur de soins est nécessaire pour obtenir des renseignements précis.

[2] L'OCDE a adopté huit principes en matière de protection de la vie privée. L'Association canadienne de normalisation et la législation canadienne (la *Loi sur la protection des renseignements personnels et les documents électroniques*) en ont dix. Les législations du Royaume-Uni, des États-Unis, de la Nouvelle-Zélande, de l'Australie et de Hong Kong sont semblables. Il n'y a pas de législation nationale en matière de protection de la vie privée aux États-Unis. La loi américaine *Health Insurance Portability and Accountability* Act considère la protection de la vie privée comme l'un des rôles de la confidentialité. The OECD adopted eight privacy principles. The Canadian Standards Association and Canadian legislation (the Personal Information *Protection and Electronic Documents Act*) identify ten. The U.K., the EU, New Zealand, Australian and Hong Kong legislation are similar. There is no national privacy legislation in the U.S.A. The American *Health Insurance Portability and Accountability Act* addresses privacy more as a function of confidentiality.

[3] Utilisé par l'industrie pétrochimique pour satisfaire aux directives environnementales : détermine les dangers potentiels de chaque composante d'une procédure et détermine la façon de traiter chaque danger.

[4] Les technologies de protection des renseignements personnels sont habituellement désignées comme des technologies d'amélioration de la confidentialité (TAC); les auteurs reprennent cette expression d'usage courant dans les brochures des fournisseurs et les sites Web.

[5] Un mandant peut être une entité physique, une procédure dans un système d'exploitation, une clé publique ou toute autre abstraction appropriée.

[6] Pour plus d'information, consultez le site http://www.cis.upenn.edu/~keynote/Papers/rfc2704.txt

[7] L'authentification peut comporter un, deux ou trois éléments : une information connue d'une personne, un objet ou une caractéristique qu'elle possède. La biométrie s'intéresse à la caractéristique que possède une personne, par exemple, l'empreinte digitale, vocale ou rétinienne. Le modèle biométrique normalisé compare une caractéristique physiologique ou comportementale d'une personne à l'enregistrement fait de cette même caractéristique. Une technologie biométrique plus poussée utilise une représentation mathématique d'une caractéristique physique, telle que la rétine, qu'elle compare à la prise d'un échantillon numérique du justificatif d'identité biométrique, la rétine. Les requêtes répétées sont pratiquement impossibles, puisqu'un échantillonnage numérique identique ne devrait pas se produire deux fois de suite ; un système peut être programmé pour rejeter la deuxième ou la troisième lecture identique consécutive.

[8] Pour chaque TAC applicable, le tableau indique le dispositif pertinent, que ce soit grâce à la conception ou à une autre méthode, telles que les politiques, la vérification, l'utilisation d'une autre infrastructure, ou à la méthode qui répond à l'exigence. Veuillez prendre note que lorsque des méthodes autres que la conception satisfont pleinement ou partiellement à une exigence, le tableau peut sembler contredire les informations des tableaux de la section 2 où seule la conception était généralement considérée.

Annexe A : Bibliographie

Généralités

Les sites Web suivants contiennent des renseignements généraux sur le respect de la vie privée ainsi que des liens à d'autres sites sur lesquels vous trouverez de plus amples renseignements. Il s'agit surtout de sites américains qui ont été créés pour assurer la protection de la vie privée.

http://www.infosyssec.com/infosyssec/anon1.htm
http://www.epic.org/
http://www.privacyinternational.org/
http://www.privacyrights.org/

Le site canadien http://www.acjnet.org/francais/index.cfm vous donne accès surtout aux lois canadiennes.
Site Web d'Industrie Canada sur le commerce électronique : http://e-com.ic.gc.ca/francais/index.html.

Site de l'OCDE : http://www.oecd.org/dsti/sti/it/secur/.

Technologie de préservation de l'anonymat

Consultez la FAQ : www.w3.org/Security/Faq/wwwsf7.html.

Voici un bon site général : www.anonymizer.com.

Le site de Roger Clarke (www.anu.edu.au/people/Roger.Clarke/DV/PEPST.html) contient des articles intéressants sur les technologies visant à améliorer le respect de la vie privée et les technologies axées sur le respect de la vie privée. Il contient aussi des renvois à d'autres articles pertinents.

Sur le site du Information Technology Industry Council (ITIC), http://www.itic.org, vous trouverez une liste des membres de ce groupe ainsi qu'un bon article sur la technologie de préservation de l'anonymat. L'article est reproduit à l'annexe B.

http://www.wired.com/wired/archive/4.05/anonymizing_pr.html
http://www.cs.du.edu/~dm/login.html
http://www.zdnet.com/zdnn/stories/news/0,4586,2682476,00.html
http://www.usenix.com/publications/login/1998-5/martin.html
http://www.research.att.com/~lorrie/pubs/networker-privacy.html
http://www.webveil.com/
http://www.wired.com/wired/archive/4.05/anonymizing.html
http://www.hicss.org/HICSS_35/hcmini.htm
http://www.securityoutpost.com/
http://www.ihtml.com/tech/internet.htm
http://mixtersecurity.tripod.com/protecting.html
http://www.sciam.com/2000/1000issue/1000techbus2.html
http://www.ntk.net/
http://www.witsa.org/news/00aug.htm
http://www-swiss.ai.mit.edu/~bianca/swiss_html/users/pmitros/privacy-proto.html
http://anon.efga.org/WebProxies
http://grc.com/downloaders.htm
http://www.lucent.com/press/0697/970610.bla.html
http://www.softouch.on.ca/rc/cookies.htm

http://www.blj8.com/Privacy/index.html
http://www.it.kth.se/~aep
http://www.eros-os.org/~majordomo/e-lang/0363.html
http://www5.zdnet.com/pcmag/stories/opinions/

Plate-forme de préférences relatives à la protection de la vie privée

Le site officiel du P3P contient l'information la plus complète : http://www.w3.org/P3P/.

http://www.cpsr.org/program/privacy/p3p-faq.html
http://www.kcoyle.net/p3p.html
http://www.w3c.org/P3P
http://www.epic.org/reports/prettypoorprivacy.html
http://www.cdt.org/privacy/pet/p3pprivacy.shtml
http://www.research.att.com/projects/p3p/
http://p3ptestbed-1.w3.org/
http://www.wired.com/news/news/story/13242.html
http://www.zdnet.com/zdnn/stories/news/0,4586,2598004,00.html
http://cobra.law.miami.edu/~jb0437/paper.html
http://www.wired.com/news/news/story/12425.html
http://www.wired.com/news/news/technology/story/13242.html
http://www.builder.com/Authoring/P3P/?tag=st.bl.3884.dir1.7584
http://www.uni-siegen.de/security/datenschutz/p3p.html
http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html
http://www.itrain.org/itinfo/2000/it000711a.html
http://www.zdnet.com/zdnn/stories/news/0,4586,2591856,00.html
http://www.w3.org/P3P/nutshell.html

Infomédiaires et systèmes de gestion de l'identité

L'article d'une page « Infomediaries and Negotiated Pprivacy Techniques », rédigé par le Dr Alexander Dix, commissaire à la protection des données et à l'accès aux renseignements de l'État de Brandebourg, en Allemagne, fait un survol des infomédiaires et des questions relatives au respect de la vie privée et à la plate-forme de préférences relatives à la protection de la vie privée. Cet article contient aussi des liens à d'autres sites pertinents. Il se trouve à l'adresse www.uni-siegen.de/security/datenschutz/p3p.html et est reproduit à l'annexe D.

http://www.consciousbuyer.com/
http://www.epsltd.com/Infomediariesmain.htm
http://www.wired.com/news/news/story/18678.html
http://www.eff.org/bayff/20010319_bayff_announce.html
http://sunsite.icm.edu.pl/sunworldonline/swol-07-1999/swol-07-bookshelf.html
http://www.wired.com/news/news/story/18217.html
http://www.thestandard.net/article/display/0,1151,17328,00.html
http://simap.eu.int/EN/pub/docs/ernst/tsld022.htm
http://www.e-commercebc.net/ic_cap_1k.html
http://www.mikealix.com/tb000913.htm
http://www.canada-ecommerce.com/ic_cap_1k.html
http://www.cyberspaceattorney.com/ezine/privacy.htm
http://www.politechbot.com/p-01079.html
http://www.gladwell.com/1999_10_04_a_sleeper.htm
http://www.cfp2000.org/news/student_reports/infomed-muller.html
http://www.junkbusters.com/ht/en/cfp.html
http://simap.eu.int/EN/pub/docs/ernst/sld022.htm

Systèmes de gestion fondée sur la confiance

L'article de M. Blaze et autres, « The KeyNote Trust-Management System Version 2 », septembre 1999, décrit en détail ce système de gestion fondée sur la confiance. Il se trouve à

l'adresse crypto.com/trustmgt/kn.html.

http://www.thethirdpower.com/index.html
http://citeseer.nj.nec.com/context/313424/23045
http://www.crypto.com/trustmgt/kn.html
http://citeseer.nj.nec.com/chu-referee.html http://www.senate.gov/~scia/hearings/730cobel.htm
http://www.cs.caltech.edu/~adam/papers/www/trust-management.html
http://www.w3.org/TR/REC-DSig-label/
http://link.springer.de/link/service/series/0558/bibs/1740/17400001.htm
http://firstmonday.dk/issues/issue3_6/khare/index.html
http://www.star-lab.com/new.html

Technologie des cartes à puce

Vous trouverez, à l'adresse smartex.com/smartcards_guide.html, une bonne explication générale de la technologie des cartes à puce. Pour en savoir davantage au sujet des cartes de réseau PC, veuillez lire l'article de Bill Lempesis, « The Future of Smart Card Technology », mars 1997, à l'adresse www.smartcardcentral.com.

http://www.scia.org
http://www.smartcard.co.uk/
http://www.mac-gray.com/
http://www.smartex.com/
http://www3.goto.com/d/sr/
http://www.fusioncard.com/
http://www.microsoft.com/windowsce/smartcard/
http://www.securenet.com.au/
http://www.tricomcard.com/
http://smart.gov/
http://www.gemplus.com/
http://www.smartcardlaundry.com/smart_cards.htm
http://www.cyberis.fr
http://members.aol.com/pjsmart
http://www.publicard.com
http://www.roaster.com/news/jul97/0728/119.html
http://www.divdyn.com/
http://www.intellect.com.au/
http://www.smartcardforum.asn.au/smartcard.htm
http://www.smartcardhelp.co.uk/
http://www.inlucid.com
http://www.smartcardcentral.com/
http://www.globalplatform.org/
http://www.lifestreamtech.com/
http://www.precis-scs.com/
http://www.tatungtel.com/main1.html
http://www.magcard.com
http://www.sfgate.com/
http://www.macgray.com/
http://www.smartdev.demon.co.uk
http://www.cs.franklin.edu/Faculty/Giuliani/mba682/~mwalter
http://smartcard.a-card.com/index.html
http://www.labcal.com/smartsign.php3
http://www.smartcardclub.co.uk/

Biométrique

Tomko, George, Ph.D., « Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy? », Privacy Laws & Business, 9th Privacy Commissioners' Data Protection Authorities Workshop, 15 septembre 1998, http://www.aliconferences.com/conferences/biometrics.htm

Une liste de développeurs et d'intégrateurs de produits biométriques se trouve sur le site biodigest.com.
Vous pouvez aussi consulter le site sur la biométrique du gouvernement américain.

The Biometric Consortium
www.biometrics.org
Créé par un groupe de fonctionnaires américains s'intéressant à la recherche sur la biométrique, ce site présente les technologies biométriques, leurs utilisations et les normes qui s'y appliquent.

Chiffrement biométrique
www.emory.edu/BUSINESS/et/biometric/
Discussions savantes sur les procédés de chiffrement biométrique, leurs usages et leurs applications

Glossaire de la biométrique 1998 (en anglais seulement)
www.afb.org.uk/glossuk1.html
Liste exhaustive de termes courants en biométrique

The Biometric Digest
webusers.anet-stl.com/~wrogers/biometrics/
Cette publication mensuelle présente les faits nouveaux dans le domaine de la biométrique. Elle contient une excellente page d'hyperliens à de nombreux vendeurs de produits biométriques.

The International Biometric Society
www.tibs.org
Cette société universitaire se consacre à l'étude des aspects mathématiques et statistiques de la biologie.

The BioAPI Consortium
www.bioapi.org
Ce groupe a été créé pour développer une interface de programmation standard pour l'application de la biométrique. Il discute de moyens d'accroître la présence de produits biométriques sur le marché.

Projet d'imagerie biométrique du Connecticut
www.dss.state.ct.us/digital.htm
Le département des services sociaux du Connecticut est en train d'intégrer la biométrique à ses procédés de prestation de services. Il pourrait constituer un modèle pour de futures applications à grande échelle.

http://biometrics.netfirms.com
http://biometrics.cse.msu.edu
http://www.precisebiometrics.com/
http://www.biom.cornell.edu/
http://homepage.ntlworld.com/avanti/
http://stat.tamu.edu/Biometrics/
http://www.zdnet.com/complife/buz/9803/biometricid-6.html
http://www.infosyssec.net/infosyssec/biomet1.htm
http://www.afb.org.uk/
http://www.biometrics.co.za/
http://www.DataCaptureBiz.com/index.asp?page=SRhome.asp&OldDate=2/01/2001
http://www.banking.com/aba/cover_0197.htm
http://www.biometrics-scan.com/
http://www.iosoftware.com/about/employment.htm
http://mason.gmu.edu/~kwong/cs103/index.htm
http://www3.goto.com/d/sr/
http://www.digitalbiometrics.com/
http://www.appliedbiometrics.net/
http://www.biometricgroup.com/a_bio1/technology/research_a_technology.htm

http://www.livegrip.com/
http://www.egroups.com/group/biometrics/
http://www.biometricpartners.com/
http://www.iris-scan.com/
http://www.tibs.org/
http://www.biometricgroup.com/

Infrastructure à clé publique (ICP)

Pour obtenir des renseignements sur l'infrastructure à clé publique du gouvernement du Canada, consultez le site Web sur l'ICP du Secrétariat du Conseil du Trésor, à l'adresse http://www.cio-dpi.gc.ca/pki-icp/index_f.asp. Vous y trouverez des foires aux questions, un aperçu de l'ICP, des politiques et des lignes directrices relatives à l'ICP et des renseignements sur la cocertification. Dans l'administration fédérale, ce site fait autorité. L'annexe H présente des exemples d'infrastructures à clé publique. Vous pouvez également consulter la page Web sur l'ICP, www.pki-page.org/, et la page de l'IETF, www.ietf.org/, qui vous renseignera sur les normes internationales en matière d'ICP.

http://www.ietf.org/html.charters/pkix-charter.html
http://verisign.netscape.com/security/pki/
http://www.itsi.disa.mil/pki/
http://oscar.dstc.qut.edu.au/
http://www.cert.dfn.de/eng/team/ske/pem-dok.html
http://www.certicom.com/
http://www.cse.dnd.ca/cse/english/gov.html
http://www.phaos.com/
http://www.pki-page.org/
http://www.counterpane.com/pki-risks.html
http://www.shym.com
http://www.rsasecurity.com/rsalabs/pkcs/index.html
http://www.authentic8.com/
http://www.infosyssec.com/infosyssec/secpki1.htm
http://www.certco.com/
http://www.usertrust.com/
http://www.pkilaw.com/
http://www.dstc.qut.edu.au/MSU/projects/pki
http://www.dvnet.com/
http://www.infoseceng.com/corppki.htm
http://www.unicert.com/library/index.html
http://www.baltimore.co.uk/
http://www.entrust.com